ARMY SCIENCE BOARD

2001 AD HOC STUDY

FINAL REPORT

DEPARTMENT OF THE ARMY
ASSISTANT SECRETARY OF THE ARMY
(ACQUISITION, LOGISTICS AND TECHNOLOGY)
WASHINGTON, D.C. 20310-0103

"KNOWLEDGE MANAGEMENT"

November 2001

Distribution Statement:
Approved for public release;
distribution is unlimited

DISCLAIMER

This report is the product of the Army Science Board (ASB). The ASB is an independent, objective advisory group to the Secretary of the Army (SA) and the Chief of Staff, Army (CSA). Statements, opinions, recommendations and/or conclusions contained in this report are those of the 2001 Ad Hoc Study Panel on "Knowledge Management" and do not necessarily reflect the official position of the United States Army or the Department of Defense (DoD).

CONFLICT OF INTEREST

Conflicts of interest did not become apparent as a result of the Panel's recommendations.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Hwy, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington D.C. 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	November 2001	**Army Science Board – 2001 Ad Hoc Study**

4. TITLE AND SUBTITLE

Knowledge Management

5. FUNDING NUMBERS

N/A

6. AUTHOR(S)

MR. JOHN H. REESE (Chair) DR. LYNN G. GREF DR. EDWARD K. REEDY
MS. CHRISTINE B. DAVIS DR. WILLIAM E. HOWARD,III MR THOMAS ROGERS
DR. JAMES R. FISHER MR. DAVID R. MARTINEZ DR. STUART H. STARR
MR. GARY GLASER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(ES)

EXECUTIVE SECRETARY
Army Science Board
SAAL-ASB
2511 Jefferson Davis Highway
Arlington, VA 22202-3911

8. PERFORMING ORGANIZATION REPORT NUMBER

N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

LTG Peter M. Cuviello
DISC4 *
(now the Army Chief Information Officer/ "G-6")
Office of the Secretary of the Army
107 Army Pentagon
Washington, DC 20310- 0107

LTG Robert W. Noonan, Jr.
Deputy Chief of Staff for Intelligence
(now the "G-2")
United States Army
1000 Army Pentagon
Washington, DC 20310- 1000

*Director, Information Systems for Command, Control, Communications and Computers

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

N/A

11. SUPPLEMENTARY NOTES

N/A

12A. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release; distribution is unlimited

12b. DISTRIBUTION CODE

A

13. ABSTRACT (Maximum 200 words)

The Army Science Board was tasked to conduct a study on “Knowledge Based Management and Information Reliability” to examine innovative ways of addressing technology issues that have the potential to “weigh down” future war-fighters with massive amounts of data. Specific subtaskings include: (1) Define Knowledge Management and Information Assurance technologies for the Objective Force; (2) Define the strategy for conquering information glut through fundamental soldier/team enabling technologies and processes from conceptual to geo-spatial; (3) Examine technology and operational concepts to mitigate asymmetric threats; (4) Provide a 2008-2012 roadmap to enable small, autonomous processing that facilitates knowledge production, sharing and decision making.

The ASB central recommendation is to incorporate and grow KM in the IBCTs. Other recommendations include: (1) Designation of KM and Info Assurance technologies as essential for Knowledge Dominance; (2) Building tactical Knowledge Management on the foundation of the existing Army Knowledge Online, the Army's excellent enterprise application; (3) Establish doctrine incorporating KM & IA technologies into Objective Force systems, including OF Combat Battalion and OF Soldier Systems; (4) Implementing a KM Center of Excellence (ARL & TRADOC); and (5) Investing in Process, Technology and Training to ensure Knowledge Dominance.

14. SUBJECT TERMS

knowledge management, information security, information assurance, communications, dissemination, Army, Army culture, information dominance, knowledge dominance, information sharing, situational awareness, network-centric, infosphere, infostructure, best business practices, networking, internet

15. NUMBER OF PAGES

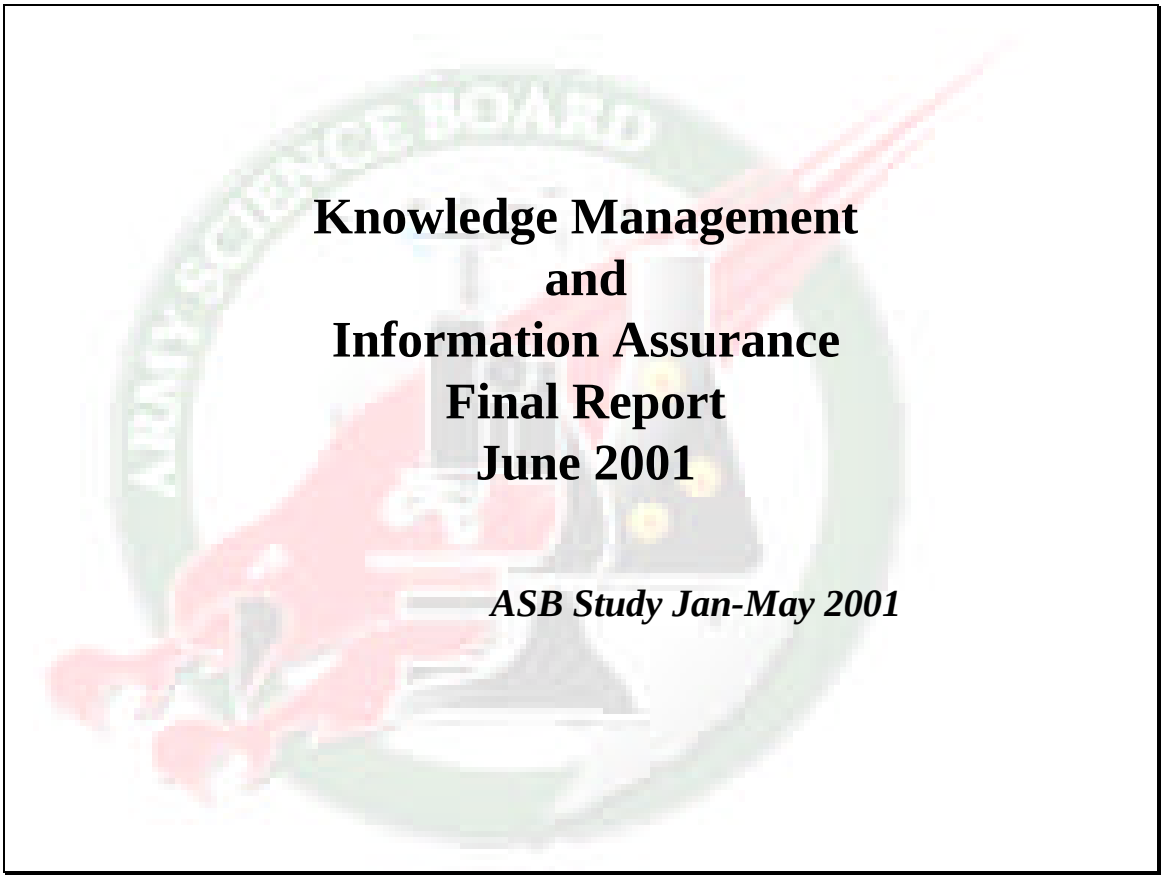
112

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THE PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	None

Knowledge Management

Table of Contents



The Knowledge Management and Information Assurance study was conducted over a four month period in 2001. The study was a short review of the current activity in the US Army and the potential for KM and IA for the future. The recommendations and findings are contained in the briefing.

The Obvious *is not* so Obvious

- **Two current examples of why Knowledge Management must be taken seriously by the US Army**
  - **War in Chechnya**
    - **A Military example – the Russians do not understand!**
  - **World Trade Center**
    - **Asymmetric Threat – We knew!**

Knowledge Management WTC "Scenario"

Knowledge Broadly Available

- WTC had been a Terrorist Target
  - Intent was to 'Topple" the two towers
  - Domestic USA was a target
- Suicide Attacks were Terrorist tool
  - Individuals
  - Teams
  - Truck Bombs
  - Small Boats
- Aircraft Hijackings were Terrorist tool
- Terrorists were capable of developing modestly complex, simultaneous events.
  - African embassy bombings

Knowledge available in selected groups

- Design of WTC against a 707
  - Architects
- Speculation of effect of a 767 collision
  - Aviation web pages in 2000
- Probability of collapse of towers
  - Architects, Structural engineers
- Unlikely an airline pilot could be forced to fly into a structure.
  - Airline pilot assoc./ Past hijackings
  - Suicide 'pilot' would be required and would need to be able to fly the plane
- US had no viable, timely response to hijacked commercial airliners if attacks occurred in tens of minutes.
  - "Defense" community
- Immigration and Naturalization Service watch list of people associated with possible terrorist activity.

3

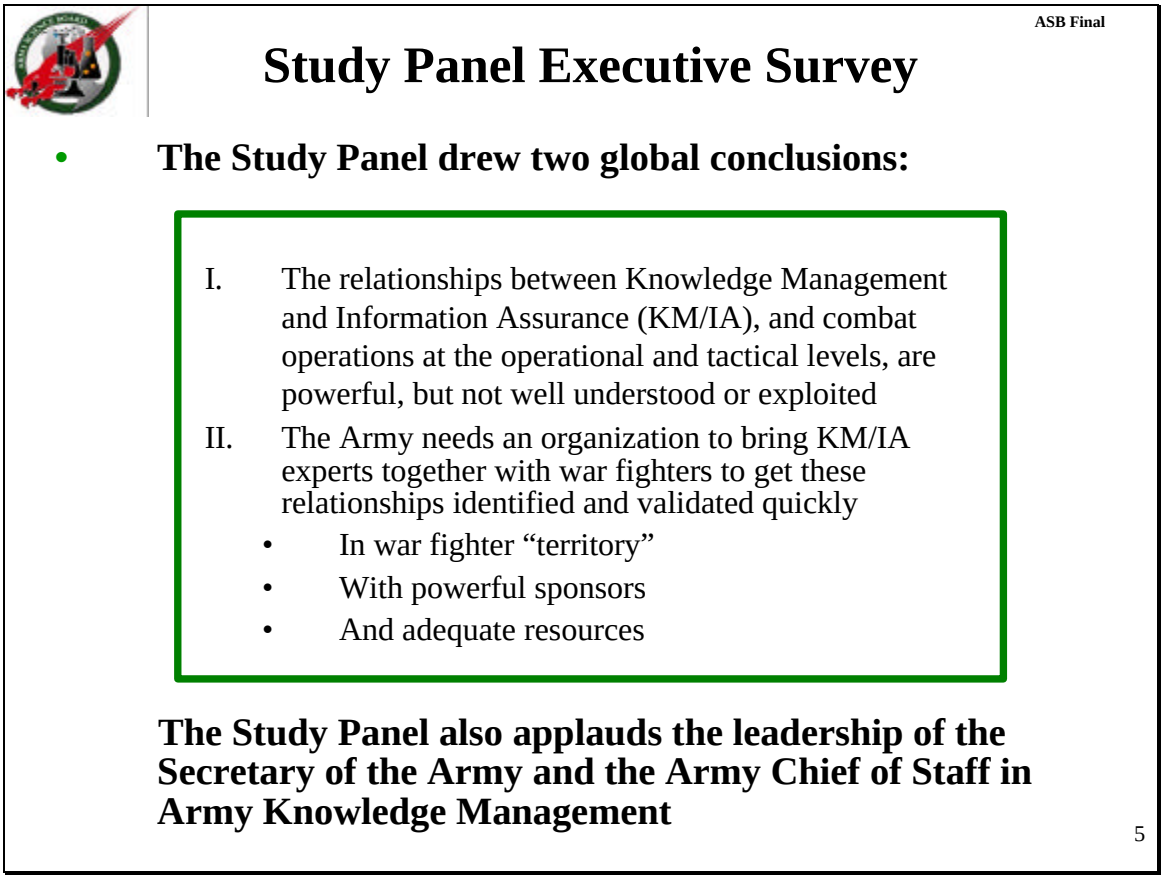
Chechen Wars*

Concerning Availability of Knowledge to Commanders:

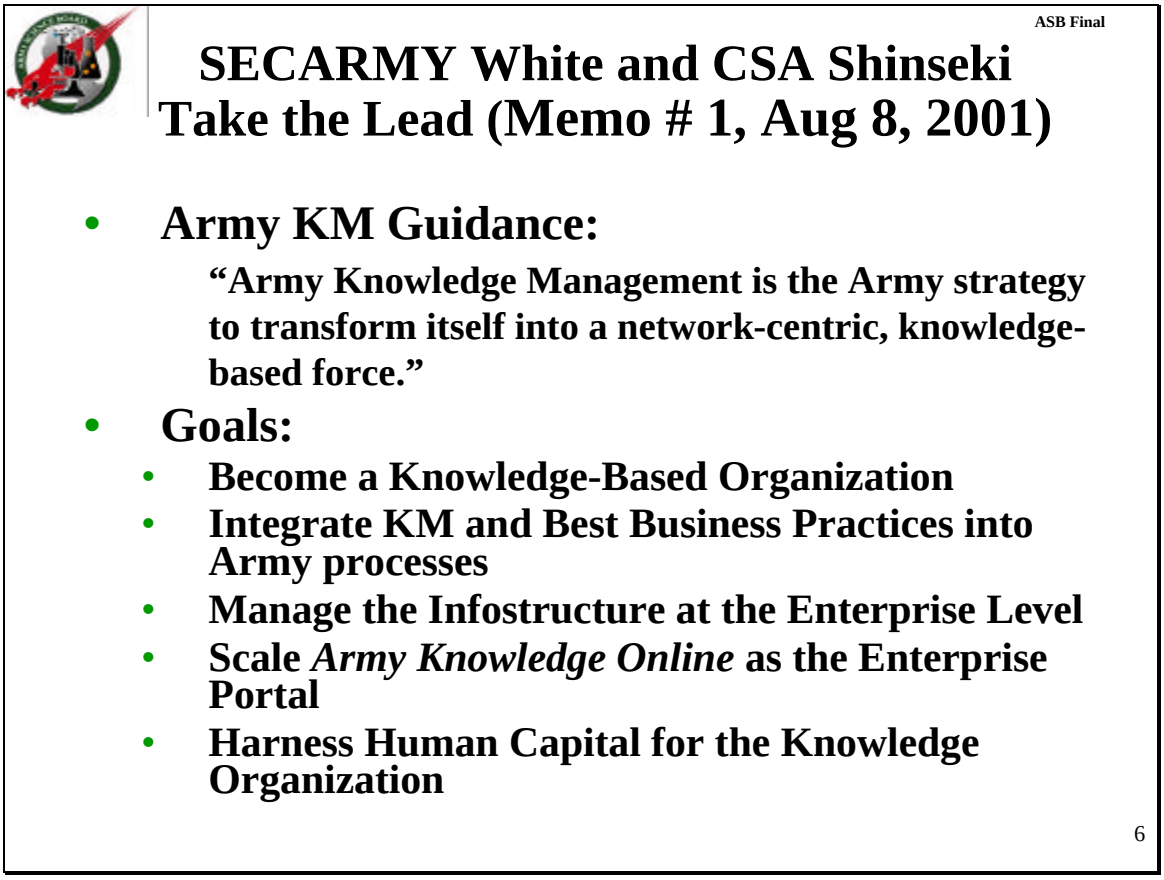
- **"Leaders were unable to transfer that knowledge to those who had to defend the city a few short months later."**
- **"Russians seem to forget painfully learned lessons from one battle to the next."**
- **"There was little effort to pass lessons learned and tactics developed on to other soldiers."**
- **"They grossly underestimated their enemy and overestimated their own capabilities."**
- **"The key mistake the Russian Military made between the wars was in drawing the wrong lessons from urban combat."**
  - **"Not only that it should be avoided."**
  - **"But that it *could* be avoided, under all circumstances."**
- **Learning under Fire: "The new leadership had a different, more systematic approach that drew effectively on lessons from the past."**
  - **"Lessons were shared."**
  - **"The rest of the force studied and copied the actions that led to success."**

Knowledge Management is the path to success with these types of issues

******Russia's Chechen Wars 1994-2000 Lessons Learned from Urban Combat*, **Olga Oliker, Rand Arroyo Center 2001**



The Study Panel drew five conclusions:
The relationship between KM and IA, and combat operations at the operational and tactical levels, is enormously powerful. However, the Army has not yet fully explored and validated this relationship. As a result, there is a vast gap in knowledge, technical understanding, field craft and even language between KM/IA experts and "muddy boots" war fighters. *The Study Panel examined this critical relationship in broad strokes, to suggest a focus for intensive Army action.*
The Army has ample experience in KM and IA in its infrastructural organizations from which to draw lessons for its war fighters.
The key to bringing KM and IA insights to bear on the Army's Objective Force is to start now with the Interim Brigade Combat Teams, rather than to start from scratch.
What is needed is a fresh "fusion" organization to put KM/IA experts and war fighters together in an intimate war fighter setting focused on Objective Force missions, doctrine, technique and procedures. The organization should be embedded in a powerful proponent organization with the institutional wherewithal and resources to make things happen quickly.
The Secretary of the Army and the Chief of Staff have to back the program.



The Study Panel notes that Secretary of the Army Thomas White and Army Chief of Staff GEN Eric Shinseki have moved out to take the KM lead. Army Knowledge Management Guidance Memorandum Number 1, published August 8, 2001, envisions a network-centric, knowledge-based force - exactly on target. There are five goals:

Adopt governance and cultural changes to become a knowledge-based organization. Hereafter, the Army CIO will lead change in all MACOM IT initiatives, through review of these initiatives by the Army CIO Executive Board.

Integrate knowledge management and best business practices into Army processes. Enhance collaborative work environments and knowledge sharing.

Manage the infostructure at the enterprise level. On October 1, 2001, Army will designate a single authority to operate and manage the infostructure at the enterprise level. Implementation will begin at MDW February 1, 2002.

Scale Army Knowledge Online (AKO) as the enterprise portal. By October 1, 2001 every soldier and DA civilian will have an AKO account. Every MACOM and functional manager must "webify" their applications and link them to the AKO by July 2002.

Harness human capital for the knowledge organization. Key to this effort is to empower people with tools and knowledge to exploit KM.

Knowledge Management and Information Assurance

Army Science Board Ad Hoc Study

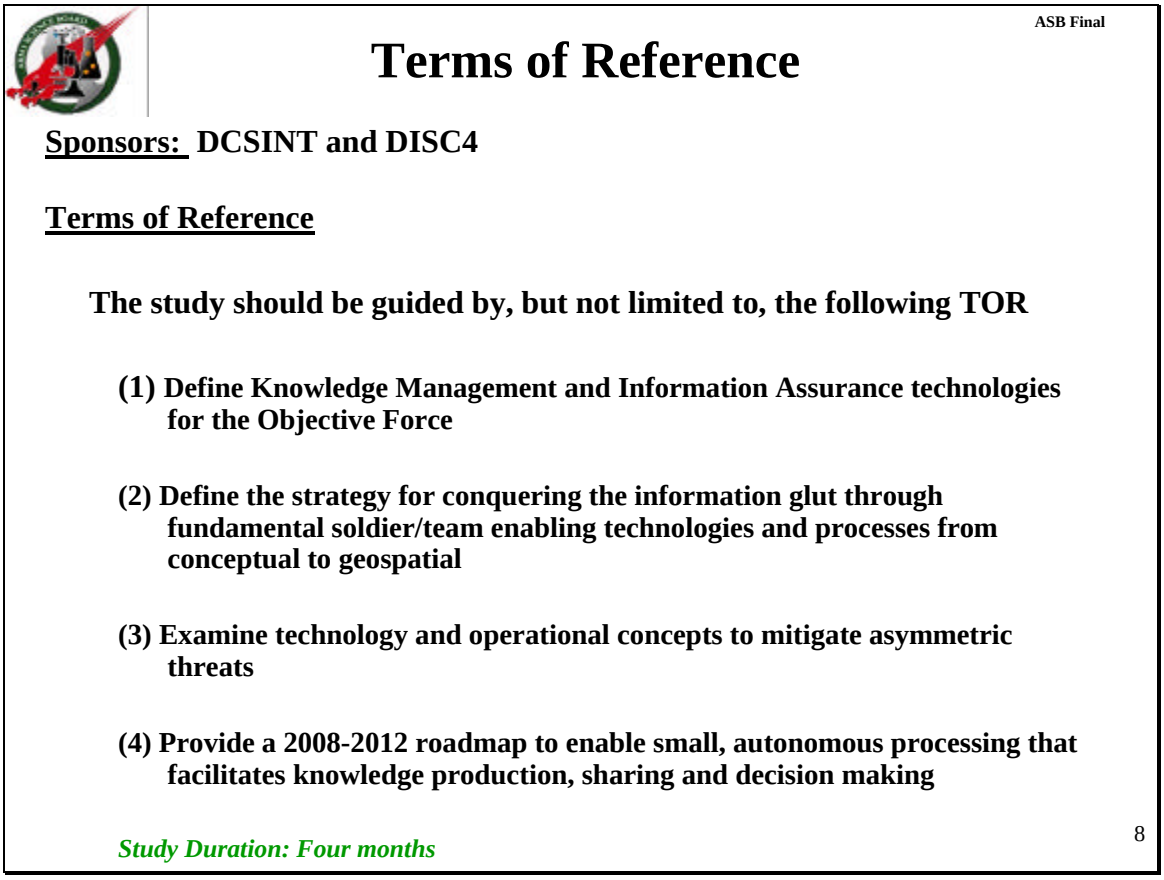
30 April 2001

John Reese, Chair
Jim Heath, Sponsor Rep.
Miriam Browning, Sponsor Rep.
Randy Woodson, Exec. Sec.

ASB Members & Consultants:	Government Advisors:	
Christine Davis	Mike Yoemans	OSD C3I
Gary Glaser	Dale Wagner	NSA
Lynn Gref	Jack Marin	USA West Point
Ed Reedy	Paul Tilson	NRO
Dave Martinez	Jack Wade	ARL/SLAD
Bill Howard	Judy Pinsky	CECOM
Stuart Starr	Thomas Rodgers	DISC4
Gary Nelson	Kevin Wheatley	DISC4
Dick Fisher		

If the US Army is to succeed and win on the battlefield of the future, It must aggressively apply good knowledge management practices by creating: a culture of confidence, trust, mutual respect and mutual support that encourages the application of knowledge capture, and a willingness to share power through shared information. Sharing knowledge will only be successful when an environment valuing knowledge is created - demand and supply - for knowledge is created. Eventually, the shared knowledge base will lead to the erosion of private power bases (S2, S3, BOS, …), as high-quality information becomes available to all..

This study was accomplished in a very compressed time frame. The panel was represented by members of industry, academia, FFRDCs, and government experts from the Army, NSA and OSD. The findings and conclusions were the result of the panel's integrated experience and a large number of briefings and interactions with numerous government and industry teams working in the knowledge management and information assurance fields. The panel met four times for 2 day sessions and several subpanels met independently.

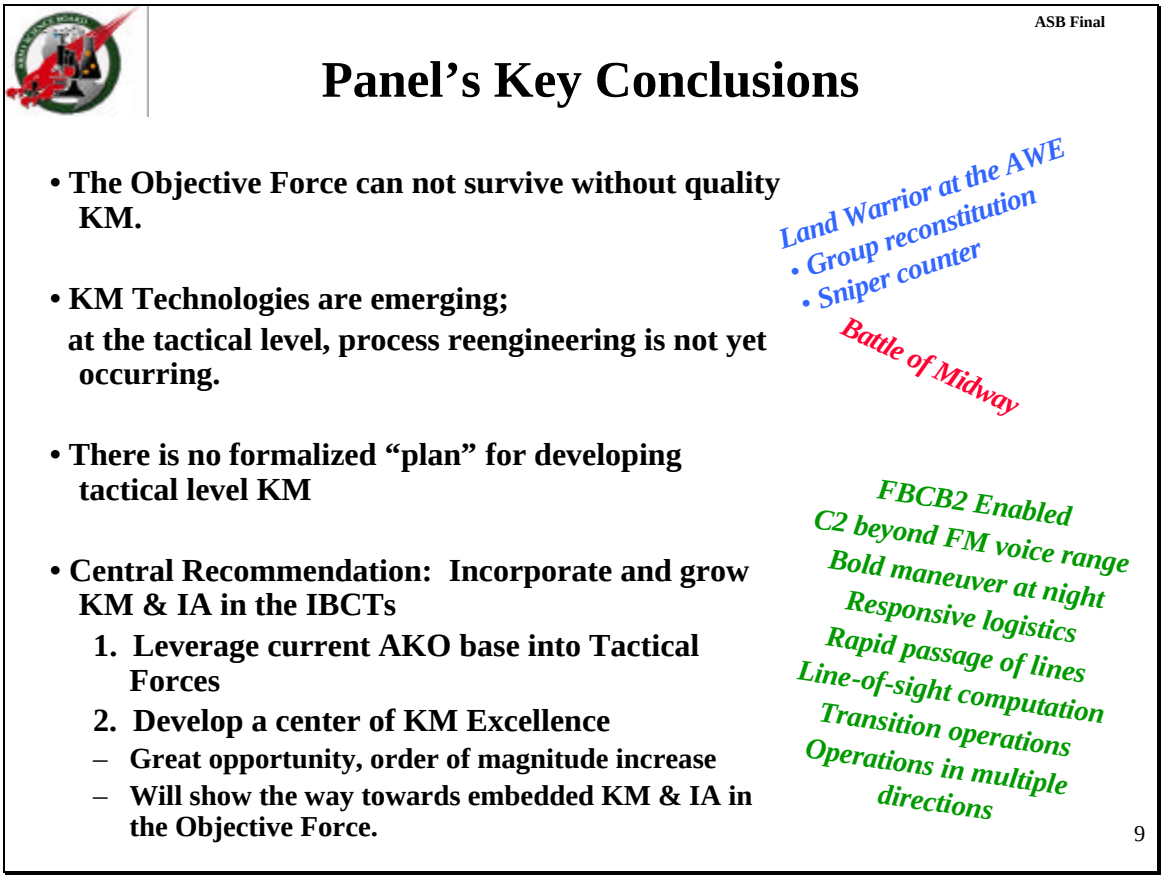


Peter Drucker first used the term knowledge management in the mid-1980s. Over the past 15 years, KM has emerged as an attempt by users to turn the deluge of information they are receiving into meaningful knowledge.

It is not a singe technology, but instead it is a collection of powerful indexing, classifying, and information-retrieval technologies coupled with methodologies designed to achieve the results desired by the user. KM's key underpinning technologies are specifically designed to run on Tactical Internet technologies. Just as they do for industry, these KM technologies enable content and workflow management, which categorize knowledge and direct it to soldiers and other knowledge workers who can benefit from it; search functionality, to let users look for relevant knowledge; and collaboration, to help soldiers share knowledge.

The Terms of Reference developed by the DISC4 and DCSINT were used to guide the panel's deliberations. Given the short study-duration of less than 4 months, the Study panel was forced deal with this broad emerging subject at a high level and to narrow the study scope to focus primarily on the Objective Force Combat Battalion. Nevertheless, the panel did become aware of some excellent Army Knowledge Management efforts at the sustaining base level. While technologies were investigated and are described, it was not possible to develop detailed roadmaps for the technologies. It is recommended that the Army Science Board maintain a subset of this panel to continue to interact with the Army to help guide the implementation of an effective Knowledge Management and Information Assurance program for the tactical levels of the Objective Force.

.



The Army investments in digitization, the future "Tactical Infosphere," quality Soldier connectivity, and new organic and Joint sensors, are all intended to provide the Soldier a superior knowledge level on the battlefield. This superior knowledge must be developed through a well engineered Knowledge Management architecture. The opportunity for orders of magnitude increases in Soldier knowledge is the basis for overwhelming battlefield dominance by future objective force. A key development which will allow the full potential of the Army investment to be realized will be the Knowledge Management and Information Assurance architecture.

Today the Army has the plans to provide the communications connectivity from and to the FCS and Soldier systems with capabilities far beyond the current forces. The Army has realized in the Strategic sustaining base level a KM architecture that supports these enterprise level activities. The KM and IA technology developed both in the commercial sectors and the Government sectors provides the tools to enable a powerful architecture for tactical forces. However the Army has not moved to develop a plan to define and embed this capability in the future force.

Incorporation and expansion of KM and IA in the IBCTs presents a great opportunity with the potential to provide an order of magnitude effectiveness increase over today's units. Knowledge superiority has always held a strong place in combat. The Battle of Midway is an example of Strategic Knowledge, but the recent AWE with LandWarrior proves that the advantage is as powerful at the tactical, squad or individual soldier level. The technology is here to give the tactical unit this advantage. FBCB2 shows the emerging potential. The Army needs to extend the focus to the knowledge management level to fully capitalize on the future potential of a knowledge superior force and help develop embedded KM and IA in the Objective Force. The current AKO KM expertise is a significant starting point to move KM into the tactical forces. Combined with the establishment of a KM "Center of Excellence" this expertise will allow the Army to successfully move KM technology into the Tactical forces. TRADOC should be designated as the lead organization in carrying out this recommendation.

KM and IA Defined

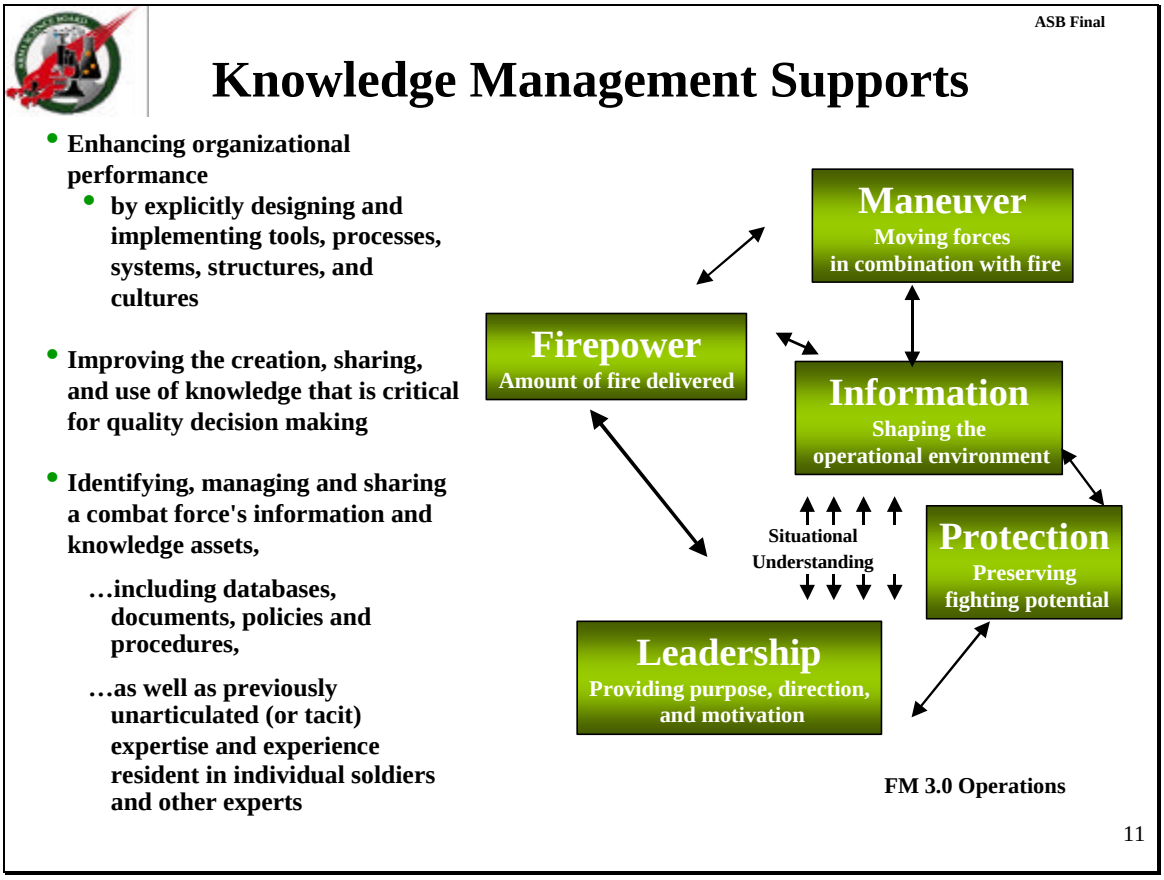
- The Study Panel found appropriate KM and IA definitions for the Study:[1]
  - ***"The purpose of knowledge management (KM) is to enhance organizational performance by explicitly designing and implementing tools, processes, systems, structures, and cultures to improve the creation, sharing, and use of all . . . types of knowledge that are critical for decision making"***
  - ***"Information Assurance (IA) is 'Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities'"***

10

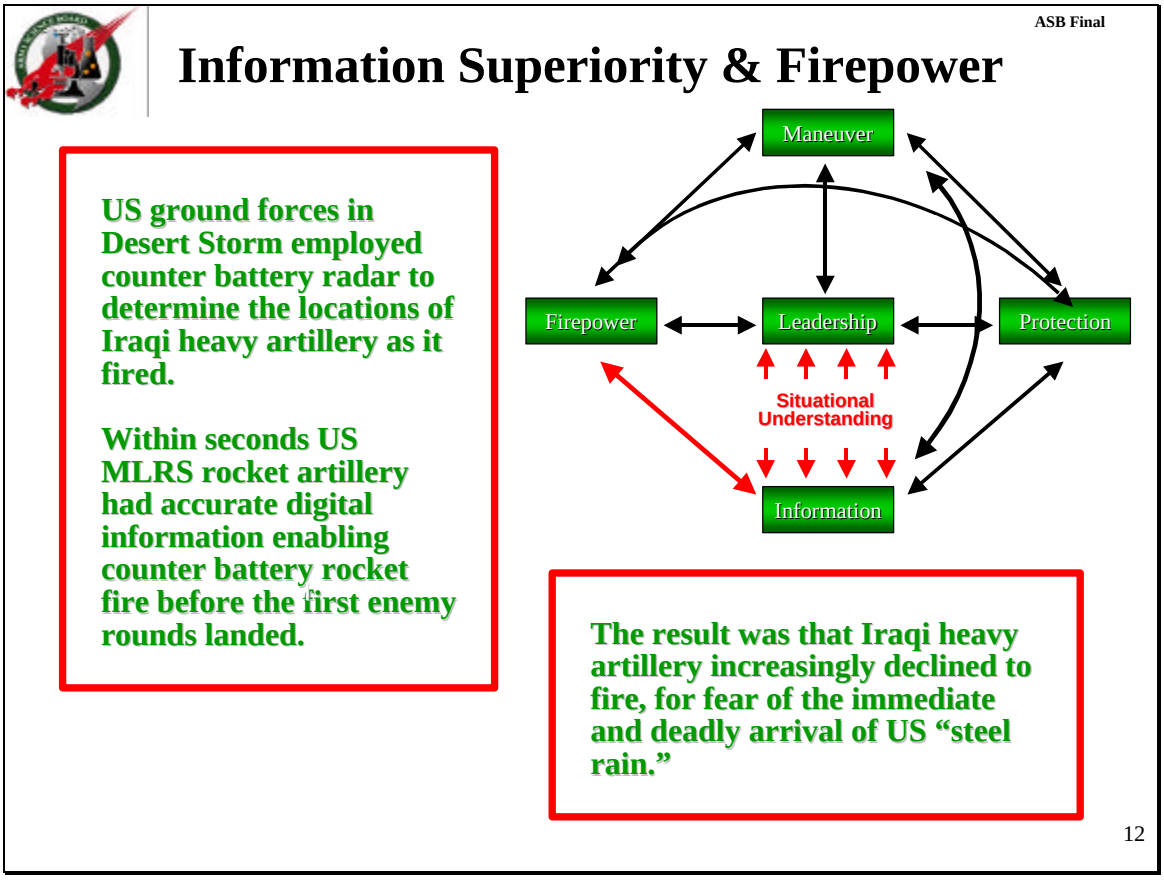
There is at present no official DoD-wide definition of KM. This definition, drawn from the Academy of Management Executives, facilitates applying KM's core elements to the war fighter's problem:
Improved organizational performance = Better creation,
sharing and use of knowledge, by integrating (tools, processes, systems, structures and cultures).

The IA definition, from the INFOSEC Glossary, is undoubtedly more recognizable to the war fighter.

Footnotes:
1. KM: "**Diagnosing Cultural Barriers To Knowledge Management," published in the Academy of Management Executives, 2000, Vol. 14. No.4, by David W. Long and Liam Fahey.**
IA: **NSTISSI No. 4009, "National Information Systems Security (INFOSEC) Glossary," January 1999.**



Evidence shows that Industry has received enormous benefits form their knowledge management initiatives over the three years. The Army is also realizing similar returns in their KM programs at the sustaining base level. **However, the real payoff to the Army of applying the verging communications, networking, and Internet technologies, which are now used so pervasively in the private sector, will come at the Combat Battalion level**. It is a certainty that the opportunity to provide timely knowledge sharing all the way to the individual dismounted soldier will exist in the "Objective Force" timeframe. Coupled with Knowledge Management, enabled by the "Tactical Infosphere" concept, Information Assurance becomes a critical requirement for the future. Without information assurance the opportunity to have an Information Dominant or Knowledge Superior force cannot be realized. As powerful information sharing moves to the Battalion and then the dismounted soldier, information assurance will be key to the ability of the unit to overmatch the enemy with superior knowledge. The communication and information flow must be secure, continuous and totally trustworthy. This will be a difficult task in the face of hostile information operations.
The purpose of knowledge management in industry is to enhance organizational performance by explicitly designing and implementing tools, processes, systems, structures, and cultures to improve the creation, sharing, and use of all three types of knowledge that are critical for decision making. Knowledge management is typically made operational through a series of new projects, (such as British Petroleum's virtual teamwork program using video conferencing to share human expertise between remote sites), processes (such as creating research teams to visit customer sites), and activities (such as interviewing potential customers).



Technology capabilities can be integrated into indirect fire weapons systems to utilize overwhelming advantages in Information Superiority.

An example is the AN/TPQ-36/37 Firefinder series of phased array ground radars. The Firefinder radars are capable of measuring the trajectories of enemy mortars, artillery and rocket projectiles seconds after they are fired. Firefinder radar computers then calculate the firing location of each tracked projectile and pass that information on to friendly artillery units. Those units are usually capable of firing at the enemy artillery before the first enemy rounds land, with great accuracy.
This very short "sensor-to-shooter" cycle made it virtually impossible for Iraqi artillery units to use "shoot and scoot" tactics to displace quickly and avoid counter battery fire. US MLRS units typically executed the counter battery missions, firing rockets with 644 very lethal DPICM submunitions.
Iraqi artillery subjected to what they called "steel rain" grew so demoralized that they frequently declined fire missions rather than accept the damage imposed.

This capability is a graphic example of using information technology to operate inside the enemy's decision cycle, with decisive effects.

ASB Final

Panel's Key Findings and Resultant Questions

- **Knowledge Management is a key enabler for the Objective Force**
  - **Tactical Knowledge-driven processes span the entire range of Tactical Forces (*Training - Deployment - Combat - Post combat) and the entire breadth of DTLOMS***
  - **The *Army Transformation* to the Objective Force *provides <u>the opportunity to engineer</u>* an integrated knowledge-driven set of tactical processes. Who is the process owner….TRADOC?**
- **The Army is a leader in Knowledge Management in the sustaining base and beginning to focus on Tactical opportunities. How can Army leverage this experience to accelerate Tactical KM….?**
- **Commercial industry is designing and developing some important processes and technology that can support Objective Force Army efforts.**
  - **The Army will need to adapt and tailor requirements and research activities to fill R&D specific voids. Potential Lead! ARL?**

13

The Army Transformation plan will result in an Objective Force with entirely new capabilities and equipment. The Objective Force will dominate adversaries not only with new equipment, but <u>also new DTLOMS processes</u>. Knowledge Management is that process that when reengineered to the needs of the objective force will provide the tactical forces dominant battlefield knowledge.

The battlefield dominance in knowledge will need to be preserved through the parallel development of robust information assurance for the tactical forces in all situations, including asymmetric threat environments.

Key Army programs at the sustaining base level, including the Army Knowledge On-line program, have aggressively been accomplished and have provided the Army an excellent base of management and engineering skills in the Knowledge Management area.

ASB Final

Some Observations Regarding Current Army *Tactical* KM Initiatives

- **Learned of many excellent, independent, small efforts focused on the Objective Force…...who's orchestrating these efforts? ….no center of expertise…….**

No Center of Expertise

WKN Warrior Knowledge Network

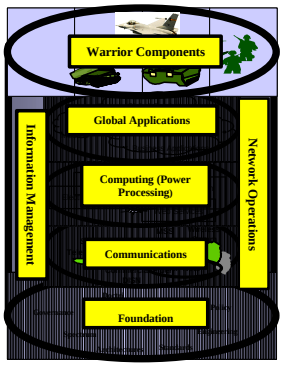
- **Initiatives @ DISC4, PEO C3S, and CALL are excellent enterprise level KM programs**
  - **Not governed by an overarching plan**
  - **Significantly under funded**
  - **Excessively focused on legacy systems**
- **Potential for engineering KM into future systems is not being considered**

- **Expansion to tactical level must be considered**

NOTE THAT -

- ***KM cannot be done well if it is not done in a system of systems construct***
- ***The information infrastructure is a critical enabler—it needs to be resourced adequately in order to be the foundation for KM***

Global Information Grid



14

The study panel was briefed by a large number of organizations and research teams. We observed numerous excellent programs and activities which will form a foundation for Army implementation of KM and IA in the objective forces. These programs are in ARL, CECOM, INSCOM, DARPA, NSA, FFRDC, Commercial industry, and, Joint experimentation areas (ACTDs and ATDs). However the programs are not being managed to a focused strategy for the objective force and most are underfunded in the panel's opinion.

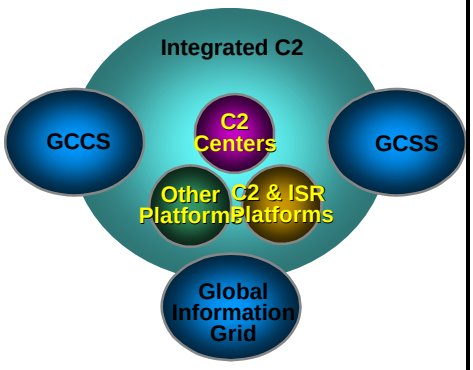
The Army, led by DISC4, has implemented excellent sustaining base programs with Knowledge Management technologies and processes. These programs are excellent efforts and leaders in the Defense community. The Army has significant leadership in the KM area in both DISC4 and DCSINT efforts. In addition the Warrior Knowledge Network effort, the ARL "Center of Excellence" proposed effort and the emerging Army ICT for Information Dominance are all excellent foundation efforts for KM and Information Assurance.

The panel's concerns are primarily the observed lack of operational architecture and future vision for knowledge management and IA at the tactical level. The strangle hold of legacy systems (sunk costs) impedes transformation to a powerful KM and IA future and obscures the need to reassess DTLOMS against the future potential of **KM opportunities.**

ASB Final

Knowledge Management Elements

Joint Battlespace Infosphere



- Information Sources
- Information Processing
- Information Exploitation
- Information Storage
- Information Dissemination
- Knowledge Development and Recognition
- Knowledge Sharing and Absorption
- Information Assurance

15

Knowledge management is closely related to information management and information technologies. The panel evaluated both the information processes and activities and the knowledge processes and activities to better understand the actual knowledge process. It is clear that knowledge driven activities occur at all the steps investigated by the panel. In fact, it is clear that the opportunity to optimally exploit knowledge technologies will require re-engineering of much of the current process.

In the appendices, the panel has described their reviews and conclusions in some detail. It was often difficult to distinguish where the appropriate conditions exist to turn knowledge into information. However, it was clear that knowledge is generated at each step and the sharing of this knowledge in a timely manner with the soldier user was the key to a battlefield knowledge advantage.

Findings and Recommendations Information Sources

ASB Final

TIMELY, SUFFICIENT KNOWLEDGE Rather Than PERFECT, LATE INFORMATION

CURRENT PROBLEM: Existing single sensor, stand-alone product development rather than a total Battlefield awareness solution which inhibits plug and play and effective data exploitation ⇨ KNOWLEDGE

CORE CAPABILITY	TECHNOLOGY	PROJECTED STATUS @FY2006*	
		Technology	Programmatics
Information Management	Intelligent Data Management	Green	Yellow
	Common Operating Picture	Yellow	Yellow
	Human Machine Interface	Yellow	Red
RSTA & INTELLIGENCE	EO, IR, Radar, RF, LIDAR Sensor's	Green	Yellow
	Micro-acoustic, Seismic Sensor's	Green	Yellow
	Sensor Fusion – Deconflict, Template	Green	Red
	Multi-sensor Fusion	Red	Red
	ATR-Detection & Recognition	Yellow	Red

SYSTEM'S SOLUTION: A system's view must be taken in developing the ISRTA support architecture and products to enable the Objective Force and the associated Individual Soldier's accomplish their defined missions.

Automated situation awareness; Targeting; Ordnance awareness.
Knowledge providing "instant" detection and location of threats.
Mix of sensors – RF location; UHF radar; SAR/MTI radar; night vision; …..
Challenges – FOPEN; urban surveillance; mine detection; sensor fusion.

*** From FY2000 Army Science Board Summer Study: ISRT Panel**

16

The sources of information for the Combat Battalion can be divided into two distinct areas. First the information generated from organic battalion sources including embedded ISR, Target Acquisition sensors, soldier observations, soldier / team reporting, battalion C2, etc. The second area is all the sources in upper echelons. The organic sources can be handled in one manner within the battalion architecture and O&O. The upper echelon sources need to be seamlessly folded in to the battalion in a manner that complements and extends the organic capability.

Organic Sources
Embed within Combat Battalion
Deploy, task and report to Combat Battalion
Support both ISR and Target Acquisition
Include Internal C2
Include CSS requirements
Team members, leaders
Upper Echelon Sources
National, Joint USAF, USN), EAC Corp, Corp, Division
Basis of IPB and all-source S.A.
Include C2 to and from Combat Battalion
Include CSS requirements
Trainers, leaders, instructors ….

ASB Final

Findings and Recommendations Information Processing

- **Relationship to Knowledge Management**
  - **Facilitates algorithms, aided processes and techniques which will enable fast information assimilation by the warfighter**
  - **RSTA knowledge should be available at the battalion level with latencies commensurate with tactical timelines**
- **Findings**
  - **ISR sensor processing and data transformation into knowledge is at its infancy for tactical use**
  - **Target evidence aggregation for positive hostile ID and precision on target can not be done with a high degree of confidence or within a short tactical timeline (less than 10 min.)**
  - **Information fusion across different linguistic sources (text, speech, video, audio) is advancing well but not available for tactical use**
  - **Knowledge "agents" with capability of autonomous data mining need significant research**
- **Recommendations**
  - **Leverage algorithms, tools, and techniques available at the strategic level for tactical use**
  - **Develop a phased approach of introducing layers of complexity at each incremental technology demonstration**
  - **Advance the ATR technology in four stages:**
    - **Preparation of Battlefield**
    - **Mission planning and replay**
    - **Multisensor tasking**
    - **Form Common Operating Picture (real-time)**

17

Needs to be near real-time to be useful for targeting
Processing near sensors supports near real-time
Multi-sensor fusion is critical to target I.D.
ATR (Automatic Target Recognition) is the "goal"
"Organic" Combat Battalion sensors will be numerous and complex (UGSs, robotic scouts, SIGINT, IMINT, HUMINT, MASINT, UAVs, FCS vehicle sensors (I2, Thermal, radar, ESM, …). Soldier sensors will include (visual, acoustic, thermal, I2, ….)
Processing to support IPB needs to be near real-time

ASB Final

Findings and Recommendations Information Exploitation

- **Relationship to Knowledge Management:**
  - **Reduce the "passing along data" for interpretation by the Warfighter and the decision maker**
  - **Reduce the "fog of war" through the elimination of redundant, irrelevant, contradictory, untimely, meaningless data or information**
- **Findings:**
  - **Information exploitation will require human analysts supported by a large infrastructure for the foreseeable future**
  - **Inadequate resources have been programmed to develop and acquire the needed information exploitation capabilities**
- **Recommendations:**
  - **Enable effective tactical Knowledge Management by enhancing:**
    - **Use of all potential sources of information**
    - **Analysts' automation aids and filters**

18

Exploitation requires analysis
By analysts (by humans, normally slow)
By algorithms (automatic, normally fast)
Exploitation serves a wide range of needs
Target Acquisition
Countermeasures
Mission planning
IPB and Situational awareness development
Training and exercise

ASB Final

Findings and Recommendations
Information Storage

- **Information storage & management includes processes, systems, and technologies for:**
  - **Creation and management of physical repositories of information**
  - **The organization of the contents to facilitate access to the knowledge needed**
  - **The distribution of the repositories and contents to specific units**
- **Findings:**
  - **The Army will need large, dynamic knowledge repositories for the Combat BN**
  - **Combat BN and soldier/ soldier team will be dependent on knowledge generated at higher echelons**
  - **The management of complex and dynamic repositories cannot be housed in the Combat BN but must be theater or other activity**
- **Recommendations**
  - **The Army should look to commercial technology, especially internet software, to provide tools and systems for managing knowledge**
  - **Define a tactical knowledge management function which will support the Combat Battalion**

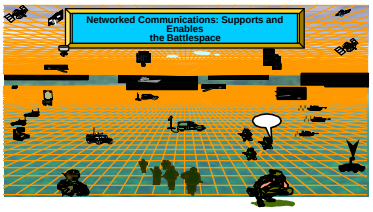
19

Information will be stored in world wide data bases and at all echelons
Access to critical information in a timely manner is a key to effective Knowledge acquisition
Information will be required in differing quality, detail and timeliness for:
Pre-Deployment IPB, Development of SA, and Planning
In-route IPB, rehearsal and mission planning
CONUS to theater
Soldier team in IFV in-route to objective
Pre-engagement updates, rehearsal
Engagement
Post engagement

Findings and Recommendations Information Dissemination

ASB Final

- **Relationship to Knowledge Management -- Key enablers of KM include**
  - **Communications with adequate capacity and resistance to adversary action**
  - **Robust, adaptive networking capabilities**
  - **The ability to get the right information to the right person at the right time**



- **Findings**
  - **Commercial information dissemination systems will provide a rich reservoir, but will not fully satisfy Army needs**
  - **Promising military information dissemination systems (e.g., JTRS, UAVs) and technologies (e.g., MOSAIC ATD, IDM-T) are emerging that could contribute substantively to improved KM … *however*, these activities are generally**
    - **Not sufficiently focused on battalion and below**
    - **Inadequately resourced**
- **Recommendations -- Provide adequate resources and focus on tactical needs in the areas of information dissemination**
  - **Systems (e.g., a more capable wideband waveform for JTRS; suitable UAVs to support communications relaying)**
  - **Technologies (e.g., extension of MOSAIC ATD, IDM-T to the tactical level; timely technology transition efforts)**

20

Relationship to Knowledge Management. Information dissemination is a key enabler for enhanced KM (i.e., necessary but not sufficient) . This implies the need for tactical communications systems that have greatly improved capacity and resistance to potential adversary action (e.g., jam resistance, LPI/LPD), networking capabilities that support enhanced adaptive network formation and sustainment, and a dissemination management capability that provides the ability to get the right information to the right person at the right time.

Findings. There will be a rich reservoir of commercial dissemination systems to draw from, but it will be limited in areas such as infrastructure base (fixed vice mobile), connections (fiberoptic, intermodal vice mobile, wireless), protection (privacy vice multiple security levels), and resistance to adverse effects (interference rejection vice robust jam resistance). There are several promising military information dissemination systems and technologies that are emerging that could contribute substantively to improved KM. These include the Joint Tactical Radio System (JTRS), unmanned aerial vehicles (UAVs), and a variety of technology initiatives at CECOM (e.g., MOSAIC ATD, DRAMA STO, IDM-T) and DARPA (e.g., SWWIM, ACN). However, these activities are generally not sufficiently focused on the needs at battalion and below and are inadequately resourced.

Recommendations. To redress these shortfalls, it is important to provide adequate resources to several key activities and to re-focus them to respond to the needs of the tactical community. In the area of information dissemination systems, there is a need to refocus JTRS to provide a more capable wideband waveform and to program adequate resources for sufficient numbers of hand-held versions. In addition, it is vital that resources be programmed to acquire and support a family of UAVs that can provide essential communications relay capability on the battlefield. In the area of information dissemination technologies, additional resources are needed to ensure that key CECOM programs are adequately supported (e.g., MOSAIC ATD, IDM-T) and broadened in scope to address key tactical concerns. In addition, additional resources are needed to build upon the innovative work that DARPA is pursuing (e.g., SUO SAS, ACN, SWWIM) and to ensure that they are transitioned to the Army in a timely fashion.

ASB Final

Information Assurance Findings

- **Information at the Combat Battalion level is the most accessible target of most adversaries.**
- **Reliable information at the "shooter" level is critical to survivability and lethality.**
  - **Unreliable information will quickly reverse the advantages of "Information Dominance" essential to force effectiveness**
  - **The panel observed a dearth of development activity at the CB level**
- **Assuring Information reliability and confidentiality in the combat battalion is difficult**
  - **close to the enemy**
  - **mobile, wireless, little redundancy, time critical sources, hostile EW, D&D, information shaping, …**
  - **detecting intrusion, jamming, deception is not enough -- must counter in real-time**
  - **failure to have IA will result in major problems for objective force units. Uncertainty, errors, delays, …….**
  - **Asymmetric threats will exist (HPM, D&D, EW, …..)**

21

The Combat Battalion will be operating in close proximity to the adversary. This proximity makes information and information systems accessible to the broadest range of attacks by the adversary. From classic EW to deception, offensive I.O., psyops, sensor degradation and confusion, the adversary will have the opportunity to degrade, disrupt, deceive, deny and destroy critical information flow. This flow will be the life blood of a information dominant force. If the information is denied or unreliable on the battlefield, US Army Information Dominance on the battlefield could be reversed.

Assuring information reliability and confidentiality will be an essential characteristic of the information systems. The architecture to Assure Information must be developed to and from the soldier up through the battalion as part of the Combat Battalion structure and to and from both lateral and upper echelon units. The bandwidth and assured connectivity and confidentiality must be such that the soldier can reliably share the required battlefield knowledge in a timely manner. This requires the Army to understand the knowledge opportunities for the objective force, develop a process driven architecture and design the information architecture to support the knowledge opportunities, not force the opportunity to live within a legacy architecture. This architecture must take into account the need for Information Assurance at all levels against a broad range of threats. In addition it will be essential to maintain an active "Red Team" activity from architecture development through the design, development, deployment, training and exercise phases to ensure robust information systems will be in place on the battlefield.

ASB Final

Assumptions and Observations Combat Battalion and the Soldier Team

- **Utilize TRADOC Unit of Action O&O from Combat Battalion to Soldier team**
- **Work Objective Force timeframe 2008 - 2015**
- **Assume Threat will identify and attack vulnerabilities of Information and Knowledge Management Systems**
- **----------**
- **A critical understanding of the organizational mission and task processes is needed to capitalize on KM technologies**
- **Recognize that sharing and collaboration are key to Knowledge Management**
- **Soldier teams will have critical knowledge to be shared, both intra team and up echelon**
- **IA is most difficult for small units in, or near contact**
- **Timelines are: Seconds to 10s of seconds in contrast to hours or days**
- **Rehearsal and pre-mission training will be a major advantage for US forces**

22

The panel attempted to focus our deliberations on the "Combat Battalion" concept. While this was not always the case, the majority of our discussion and the resultant findings and recommendations are in this context. It became obvious to the panel that the key to successful Assured Knowledge Dominance will require the Army to have a good understanding of the threat to this force's information and knowledge management systems. A deep understanding of the combat battalion mission and task processes (business processes) and a recognition that sharing and collaboration are essential to the increased survivability and lethality of the the combat battalion. This is primarily the charter of TRADOC and places a premium on the early development of these products form TRADOC.
The inclusion of Information Assurance in this process is essential, and much of the material the panel heard leaves doubt in our minds as to the emphasis of IA development focus on the tactical unit of action.

ASB Final

Phases of Knowledge Sharing

Combat Battalion Phase	Time to accomplish sharing	Data rate available to support	Presentation environment	Typical Functions Supported
Pre Deployment / Garrison	Weeks to Days	Giga bits / second	Large scale virtual reality	?? IPB ?? Planning ?? Rehearsal ?? Training
Deployment – air / ground	Days to Hours	10s of Megabits / second	Medium scale virtual reality	?? IPB updates ?? Rehearsal ?? Planning ?? Options
Assault / combat	Hours to Minutes	100s of kilobits to a megabit	Soldier carried devices	?? Mentoring ?? R/T collabor. ?? IPB updates ?? Decision aid
Post assault / recover	Hours to Minutes	A few Megabits / second	Medium scale virtual reality	?? IPB updates ?? Attack Asses. ?? Lessons learn.

23

The opportunity to share knowledge with tactical forces covers a broad spectrum of situations and activities. It is critical that the knowledge management context be developed to best support the soldier across this entire spectrum. The tools and technologies of Knowledge Management and Information Assurance need to be architected into a system which can provide the power of knowledge sharing in a complete and consistent flow across all these activities.

Much benefit can be accrued by the soldier while in garrison or pre-deployment from a well engineered Knowledge Management system. Training, rehearsal, mentoring, threat assessment, tactics review, peer discussions, expert support, IPB review and assessment all can be enhanced with a good knowledge sharing architecture. The communications connectivity at this time will be capable of supplying a wealth of knowledge to the soldiers and leaders concerning areas of interest. A smart “Portal” can make this a powerful new tool for tactical units in garrison.

Similarly during the deployment phase, the assault / combat phase and the post assault phase a good knowledge management concept will provide the right knowledge to the warrior at the time he needs it to best accomplish his mission. Sharing across peers, with experts, with mentors for both warriors and leaders will provide substantial value.

Key Technologies

- **Knowledge Management**
  - **Sharing - collaboration**
  - **Data base access**
  - **Display**
  - **Modeling and simulation**
  - **Virtual rehearsal**
  - **Information timeliness**
- **Information Assurance**
  - **Link Integrity**
  - **High speed, Survivable Networks**
  - **Secure and authenticated information**
  - **Correlation (fusion) of information sources**
  - **Hardening of hardware**

24

A broad range of technologies are associated with the emerging area of Knowledge Management. Similarily Information Assurance continues to be an exploding area of both commercial and Government technology. It will be essential for the Army to have a KM / IA center of Excellence to review and monitor these rapidly developing technologies and provide the Army program managers and TRADOC concept requirements developers a point of reference.

Key Technogies include:

Knowledge Management

Modeling and simulation: Essential to provide tools to the soldier to use knowledge and an assessment tool to evaluate tradeoffs in developing KM and IA architectures

Virtual rehearsal: A powerful new opportunity to allow the soldier and leaders to capitalize on superior knowledge prior to assault phase.

Data base access: The availability and importance of World wide data bases will require immediate and 'smart' access. The GIG should be viewed as the key enabler.

Sharing - collaboration: This is the key technology of Knowledge Management and the key operation that must be secured by IA. The technologies for sharing include browsers, intelligent agents, Portals and other internet technologies

Display: Displays for soldier in combat or in garrison need to move towards an embedded neural concept. The future holds much promise to provide a US Army Warrior a real advantage on the battlefield if knowledge can be effectively imparted to him with displays

Information Assurance:

Link Integrity: Continuous connectivity will be essential to fully exploiting the US information and knowledge advantage. The links must be both reliable and assured. Much of this technology will be developed in the commercial community, but key elements will be required to be developed in the ISSO environment

High speed, Survivable Networks: The DARPA work on SUO SAS is an excellent step in the right direction for a tactical network designed to survive and function in a hostile environment. This process needs to be moved into future Army tactical information architectures.

Secure and authenticated information: It will be essential to work with NSA to ensure that the rich content of the future Army networks remain secure and that the user can trust that the data is authentic.

Correlation (fusion) of information sources: A critical area where major opportunities exist to apply commercial products and where significant Army/ DOD R&D will be required

Hardening of hardware: Like software vulnerabilities the hardware associated with connectivity and knowledge dissemination and use will need to be hardened against classical EW and IO techniques as well as battlefield attacks associated with HPM and physical capture of elements of a network.

ASB Final

Technologies

Technology Readiness Levels

Enabling Technologies	2004	2008	Commercial
Aided ATR	3	3	2
Smart Portals to push pull	6	9	9
Mobile Wireless (pagers, PDA)	6	9	7
Malicious Mobile Code	1	2	3
Visualization - Presentation	4	7	6
Data Extraction	6	8	8
Virtual environment	3	6	6
Automatic routers, priorities	5	8	5
Data fusion, information fusion	2	3	
Secure Intelligent Agents	2	5	7
Encryption and authentication	4	7	6
Exploitation Algorithms and assist	2	2	2
RTIC	5	8	
Future Internet	6	9	9
Individual Soldier Tech.	4	8	5
Collaboration Technologies	6	9	8
Sync Distributed Secure Data base	4	7	5
Secure Access Technology Biometrics	3	8	5
Translingual language transcription	4	6	7
Soldier Education	6	8	7
Associates	6	7	5
Next Generation Internet	6	9	9

TRL=Technology Readiness Levels

Commercial- % commercial R&D (1-10)

26

Technology Readiness Levels and Their Definitions

Technology Readiness Levels

1. Basic principles observed and reported.
2. Technology concept and/or application formulated.
3. Analytical and experimental critical function and/or characteristic proof of concept.
4. Component and/or breadboard validation in laboratory environment.
5. Component and/or breadboard validation in relevant environment.
6. System/subsystem model or prototype demonstration in a relevant environment.
7. System prototype demonstration in an operational environment.
8. Actual system completed and 'flight qualified" through test and demonstration.
9. Actual system 'flight proven" through successful mission operations.

These are described on the next page.

Technology Readiness Levels and Their Definitions

Technology Readiness Level	Description
1. Basic principles observed and reported.	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated.	Invention begins. Once basic principles are observed, practical applications can be invented. The application is speculative and there is no proof or detailed analysis to support the assumption. Examples are still limited to paper studies.
3. Analytical and experimental critical function and/or characteristic proof of concept.	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment.	Basic technological components are integrated to establish that the pieces will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of 'ad hoc' hardware in a laboratory.
5. Component and/or breadboard validation in relevant environment.	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. Examples include 'high fidelity' laboratory integration of components.
6. System/subsystem model or prototype demonstration in a relevant environment.	Representative model or prototype system, which is well beyond the breadboard tested for TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high fidelity laboratory environment or in simulated operational environment.
7. System prototype demonstration in an operational environment.	Prototype near or at planned operational system. Represents a major step up from TRL 6, requiring the demonstration of an actual system prototype in an operational environment, such as in an aircraft, vehicle or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and “flight qualified” through test and demonstration.	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system 'flight proven" through successful mission operations.	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. In almost all cases, this is the end of the last "bug fixing" aspects of true system development. Examples include using the system under operational mission conditions.

ASB Final

ASB Recommended Tactics

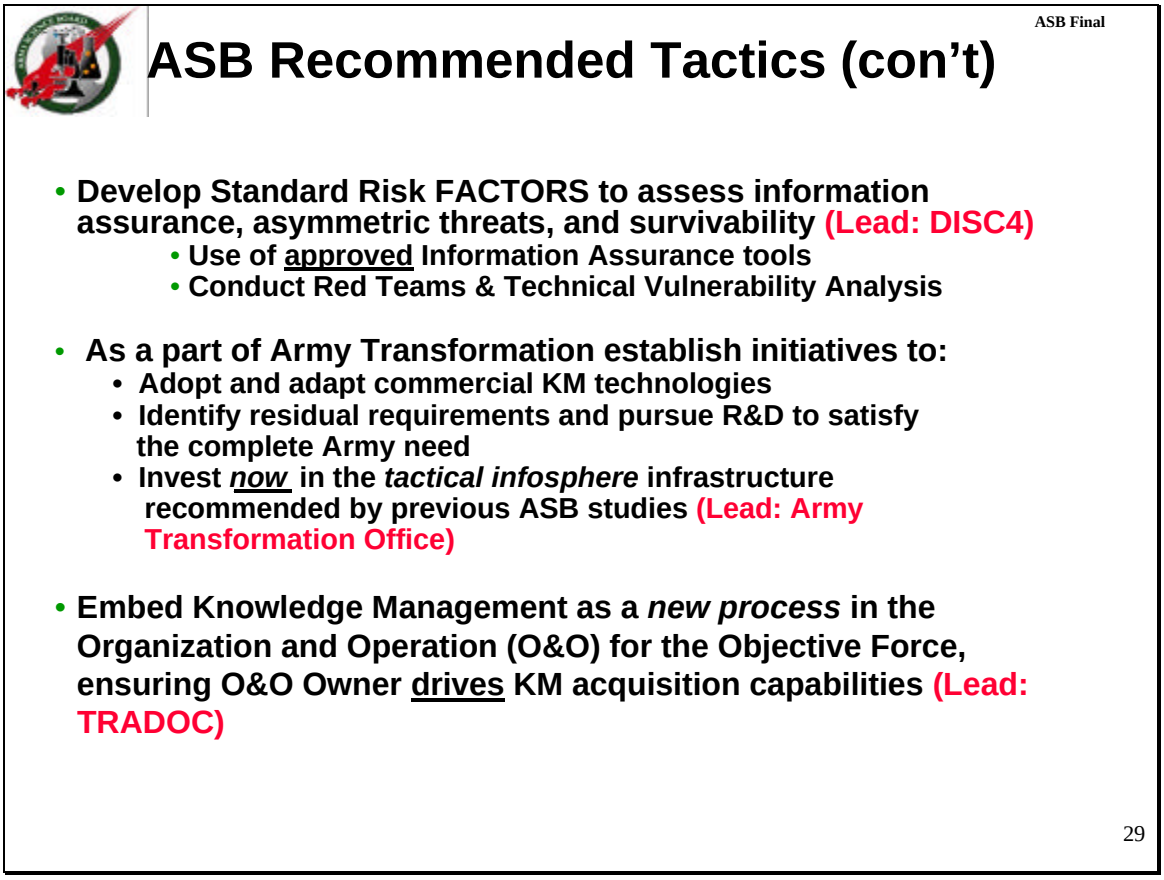
- **Designate Knowledge Management and Information Assurance technologies as essential to Army *Knowledge Dominance* *(Lead: CSA)***
  - **..and the opportunity to degrade the enemy's Knowledge Management system - Counter Knowledge Management (Lead: DCSOPS)**
- **Build tactical level Knowledge Management on Army's excellent enterprise applications – e.g., Army Knowledge Online (Lead: DISC4)**
- **Write new Army doctrine requiring developers to integrate Knowledge Management and Information Assurance technologies into the design and development of Objective Force Combat Battalion and Soldier Systems. (Lead: TRADOC)**
- **Implement: *(With ARL and TRADOC)***
  - **A "Center of Excellence" for Army combat applications of KM**
  - **An integrated plan for Information Assurance, including a strong technical and operational "Red Team"**
- **Invest in Process, Technology and Training to ensure Army tactical forces have *Knowledge Dominance* *(Lead: TRADOC)***

28

Assured Knowledge Dominance needs to be acknowledged by the Army leadership as a primary objective of the objective force. While the Army has done a magnificent job of building the information dominance image, this has not resulted in the message of knowledge sharing as the enabler of the future. The culture still regards knowledge owning as power, not knowledge sharing as power. This culture will need to be changed, as it has been in industry reengineering, in Army sustaining base programs, and in the OSD C3I programs, to move to a culture where the rewards are for the sharing not the owning.

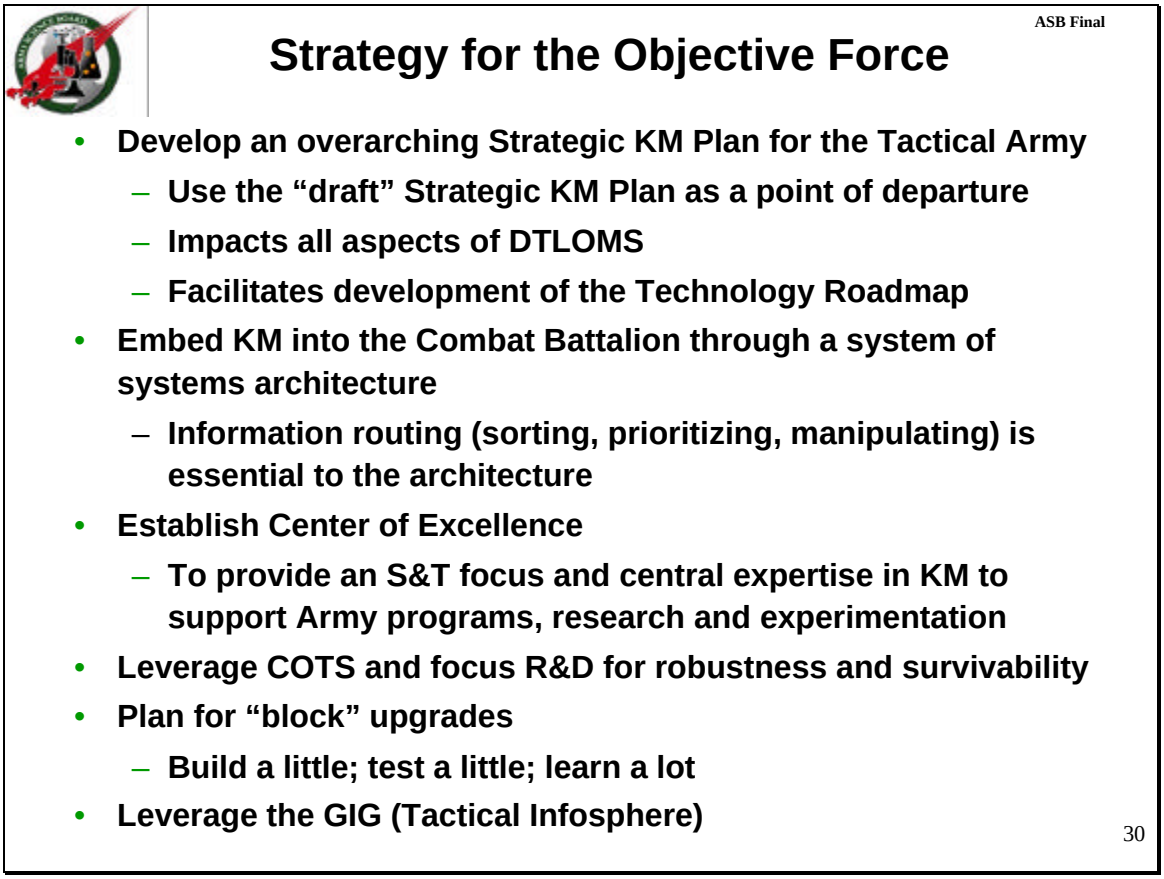
This change requires the O&O for the objective force to reflect this cultural change. That the infrastructure to enable sharing be implemented not only in the combat situation, but in garrison, in deployment and in recovery phases. It requires that the implementation place emphasis on the assured connectivity of knowledge communities, without which the combat soldier will never be able to rely upon the power of sharing. The change of culture will require extensive training and exercise and strong, committed leaders to move into the opportunity that knowledge management will provide.

The majority of the technology will be developed by the commercial industry, but it will be essential for the Army to have an active R&D program to capitalize on the commercial investments and tailor these to Army applications.



Risk management is essential to the objective force and will be critical in this area of Assured Knowledge Dominance. Failure to build a robust system will result in loss of all the benefits the Army plans to obtain from Information Dominance. Therefore it is strongly recommended that the Army build a life cycle capability to Red Team through the entire concept to deployment cycle the Assured Knowledge Management capabilities. This might be accomplished by extending the role of the ICT being developed by the Army for the Tactical Infosphere assessments.

Process is key to the successful development of powerful Knowledge Management applications. Industry has time and time again shown this to be true. The Army's successful Knowledge Management programs at the sustaining base level prove this to be true as does the OSD/C3I program. The Warrior Knowledge Network program is a good start at understanding the Objective force process. However most critical is an owner of the process. This should be TRADOC, with a "Center of Excellence" providing a basis of the resultant architecture(s) needing development.

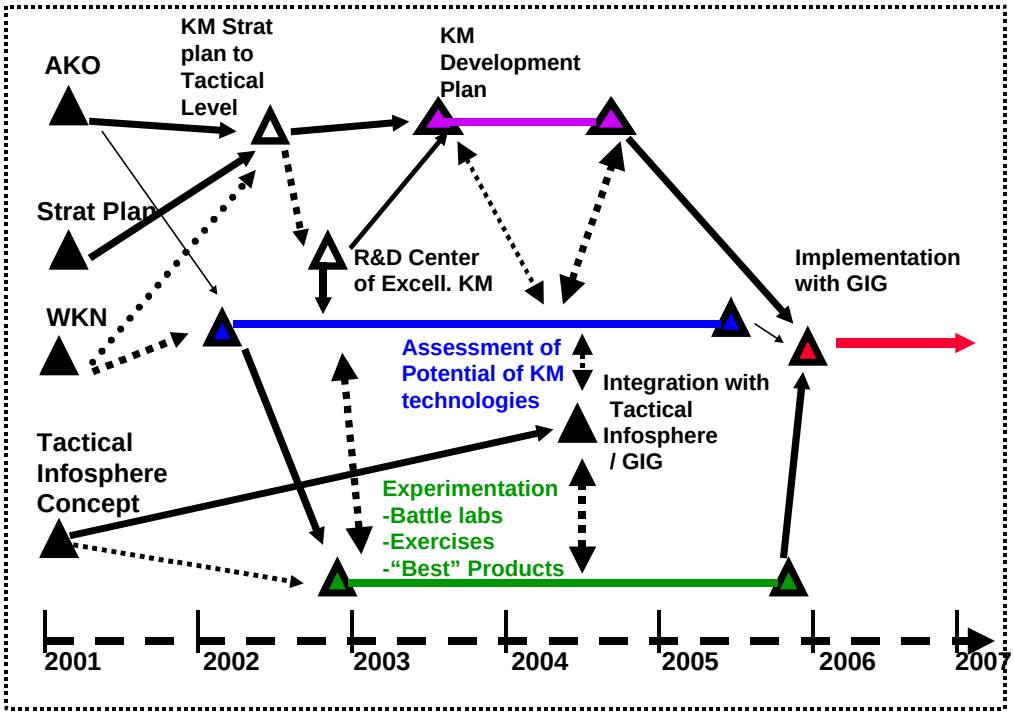


Develop an overarching Strategic KM Plan for the Tactical Army. The initial step should be to use the Army "draft" Strategic KM Plan as a point of departure. This provides an excellent opportunity to build a Strategic-Tactical KM plan for the future. It is important to recognize that KM will impact all aspects of DTLOMS> This should be taken into account early and TRADOC needs to begin to accommodate the vision of a Knowledge Superior Warrior. With the draft plan developed, it will facilitate the development of the Technology Roadmap. This roadmap will be based primarily on the KM tools and products developed in the commercial center and applied to Army tactical applications. The intent needs to be to embed KM into the Combat Battalion through a system of systems architecture. This systemof Systems concept should be able to correlate the Army knowledge sharing concept from National to dismounted soldier and squad to Joint. The key Army enablers will be;

1. Digitization and the "Tactical Infosphere
2. The GIG and related communications connectivity and distributed databases
3. The Army change of policy to demand and reward the change to a culture of knowledge sharing.

In order to immediately begin to demonstrate the value of the KM opportunity, it is important to establish Center of Excellence within the Army. The objective of this Center of Excellence will be to provide an S&T focus and central expertise in KM to support Army programs, research and experimentation. The Center would also provide a central organization to focus and leverage COTS and ensure R&D for robustness and survivability. Plan for "block" upgrades of current and programmed IT and KM systems and lead in the development of a build a little; test a little; learn a lot experimentation approach to move KM and IA into the objective force. It cannot be overstated that this is the opportunity to leverage the GIG (Tactical Infosphere) and develop an architecture that does not route information, but instead builds a knowledge sharing and knowledge acquisition vision to ensure the superiority of the US Army soldier on the future battlefield.

Technology Roadmap



All DTLOMS are affected by Knowledge Management

ASB Final

DOCTRINE:

KM will neccessitate new doctrine for the Combat units

TRAINING:

KM will enable dramatic opportunities to improve training

LEADERSHIP:

Leadership will be able to more effectively leverage soldiers capabilities

ORGANIZATION:

KM will provide the opportunity for different organizational "communities"

MATERIEL:

KM enables the development of a broad range of new objective force systems and tools

SOLDIERS:

Soldiers will become more knowledgeable, more aware, more decisive, more lethal and more survivable

POLICY:

The policies (business rules) of knowledge sharing among soldier and soldier support communities will be dramatically different from today

32

The panel recognized that both Knowledge Management and Information Assurance are solutions that can and will directly impact all areas of the Army DTLOMS. The move to an Army Knowledge management architecture will change much of the hierarchical information dissemination and access structure that was limited by the communication and knowledge dissemination technologies of the past. As Portals, Browsers and high quality network connectivity become available to the soldier, many of the restrictions of the past will be eliminated. Peer to peer real-time communications enable a totally new level of knowledge sharing. Access to experts, mentors and Worldwide databases provide new paradigms of operations for leaders and soldiers- not only in training and rehearsal. But in combat operations. The totality of DTLOMS and policy will need to be "adjusted" to accommodate the Knowledge Superior Warrior of the Objective Force.

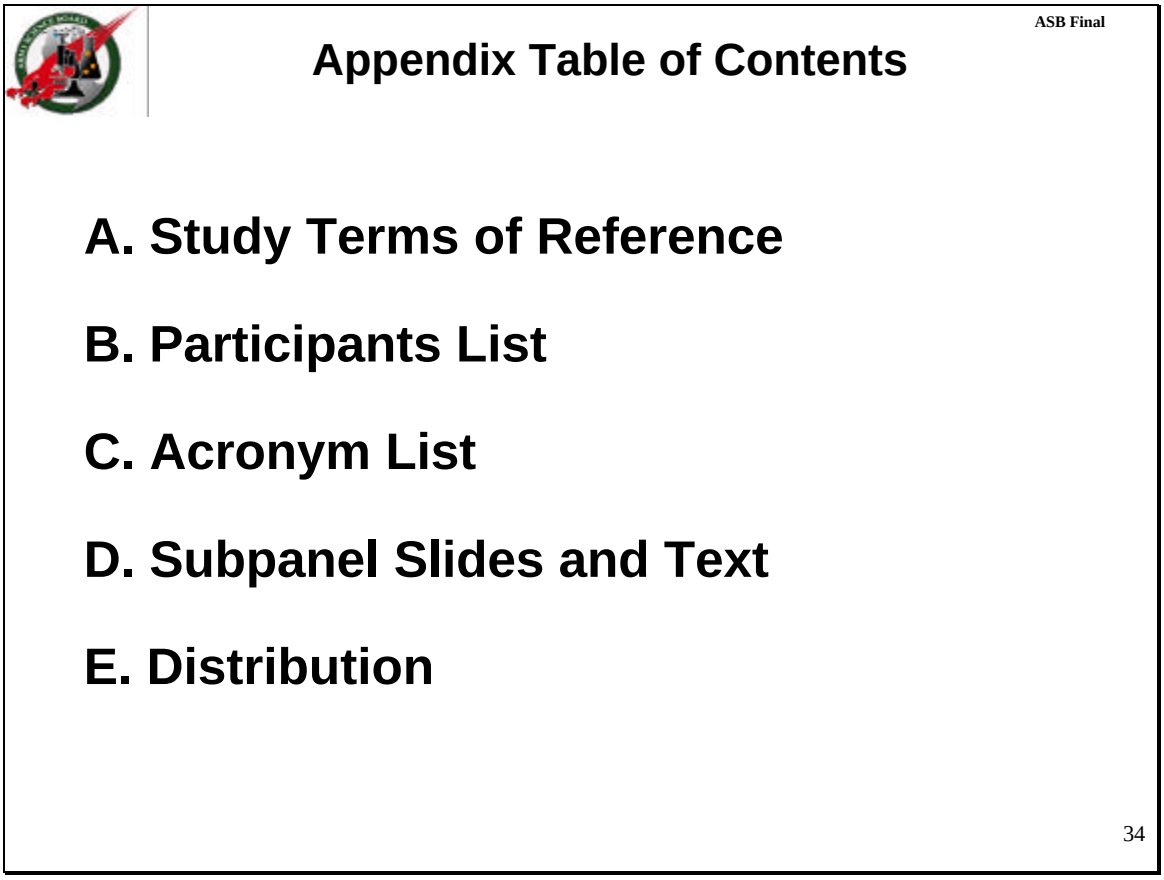
What Could the ASB Do Next?

- **Support development of the:**
  - **High level system architecture**
  - **Technology roadmap**

1. **ASB work with TRADOC and key Army offices (e.g.ARL-Center of Excellence, CAC (WKN), Info Dominance Center and DISC4 AKM Strategic plan) to develop a construct for KM in the Objective Force Combat Batalion.**
2. **ASB continue to develop KM opportunities as part of on-going summer Study**
3. **Brief results to Army and OSD leadership**

33

A necessary step to move forward with this opportunity is the development of a high level strawman architecture. The panel believes they could contribute to this effort and in conjunction with TRADOC and CAC provide a excellent piece discussion for the Army. This would include both a high level systems architecture and a technology roadmap to reach a 2012 goal of a optimized Knowledge management and Information Assurance solution for the objective force Combat Battalion



The panel developed an extensive understanding of the KM and IA technology areas. This data is captured in Appendix D which consists primarily of viewgraphs on the subjects reviewed.

APPENDIX A

TERMS OF REFERENCE

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
ACQUISITION LOGISTICS AND TECHNOLOGY
103 ARMY PENTAGON
WASHINGTON DC 20310-0103

REPLY TO
ATTENTION OF

December 28, 2000

Mr. Michael Bayer
Chairman, Army Science Board
2511 Jefferson Davis Highway, Suite 11500
Arlington, Virginia 22202

Dear Mr. Bayer:

I request that the Army Science Board (ASB) conduct a study on "Knowledge Based Management and Information Reliability" to examine innovative ways of addressing technology issues that have the potential to "weigh down" our future warfighters with massive amounts of data. The study should address, but is not limited to, the Terms of Reference (TOR) Described below. Appointed ASB members to this study are to consider the TOR as guide lines and may expand the study to issues considered important to the study. Modifications to the TOR must be addressed with the Chairman of the ASB.

Background:

a. Information dominance will provide the underpinning of Objective Force Operations. Future adversaries will have access to advanced commercial information technology that can and will be used to asymmetrically disrupt United States operations. Therefore, it is imperative that our Forces have the adequate information assurance technologies that will enable relevant, reliable and easily understood information at all levels. Technology must be applied in the right mix to prevent weighing down our soldiers with an information glut that only adds more friction and confusion to the warfight.

b. I envisage that this study will identify potential knowledge management and information assurance technologies that will provide the future warfighter with relevant, reliable and easily understood information. The study should highlight science and technology opportunities that Army Leadership can exploit through a focused research, development and acquisition effort.

TOR: The study should be guided by, but not limited to the following TOR.

(1) Define Knowledge Management and Information Assurance technologies for the Objective Force.

Printed on Recycled Paper

(2) Define the strategy for conquering the information glut through fundamental soldier/team enabling technologies and processes from conceptual to geo-spatial.

(3) Examine technology and operational concepts to mitigate asymmetric threats.

(4) Provide a 2008-2012 roadmap to enable small, autonomous processing that facilitates knowledge production, sharing and decision making.

Study Sponsorship: Co-Sponsors for this study will be Deputy Chief of Staff for Intelligence and Director, Information Systems for Command, Control, Communications and Computers.

Study Duration: The study shall be completed by April 30, 2001.

Sincerely,

Paul J. Hoeper

Paul J. Hoeper
Assistant Secretary of the Army
(Acquisition, Logistics and Technology)

APPENDIX B

PARTICIPANTS LIST

PARTICIPANTS LIST
ARMY SCIENCE BOARD 2001 AD HOC STUDY

KNOWLEDGE MANAGEMENT

ASB Panel

Mr. John Reese, Study Chair
Private Consultant

Ms. Christine Davis
Executive Consultant

Mr. Gary Glaser
DIA Advisory Board

Dr. Lynn G. Gref
Jet Propulsion Laboratory

Dr. William E. Howard, III
Private Consultant

Mr. David Martinez
MIT Lincoln Laboratories

Dr. Gary R. Nelson
Private Consultant

Mr. James R. Fisher
DESE Research, Inc.

Dr. Stuart Starr
The MITRE Corporation

Gov't Advisors

LTC Jack Marin
U.S.M.A., West Point

Ms. Judy Pinsky
CECOM

Mr. Thomas Rogers
DISC4

Mr. Paul Tilson, Jr.
NRO

Dr. Jack Wade
ARL/SLAD

Mr. Dale Wagner
NSA

MAJ Kevin Wheatley
DISC4

Mr. Mike Yoemans
OSD C3I

Staff Assistant

Mr. Randall Woodson
ODCSINT

Sponsors

LTG Robert W. Noonan, Jr.
Deputy Chief of Staff for Intelligence

LTG Peter M. Cuviello
Director of Information Systems for Command, Control, Communications and Computers

Sponsor Representatives

Mr. James Heath
ODCSINT

Ms. Miriam Browning
ODISC4

APPENDIX C

ACRONYMS

ACN	Airborne Communications Node
ACTD	Advanced Concepts Technology Demonstration
AKO	Army Knowledge Online
ARL	Army Research Laboratory
ATR	Automatic Target Recognition
AWE	Advanced Warfighting Experiment
C2	Command and Control
C3S	Command, Control, and Communications Systems
CAC	Combined Arms Center
CALL	Center for Army Lessons Learned
CB	Chemical-Biological
CECOM	Army Communication-Electronics Command
CIO	Chief Information Officer
CONUS	Continental United States
COTS	Commercial off-the-shelf
D&D	Denial and Deception
DARPA	Defense Advanced Research Projects Agency
DCSINT	Deputy Chief of Staff for Intelligence (outdated, now DCS G-2)
DISC4	Director of Information Systems for Command, Control, Communications, and Computers
DoD	Department of Defense
DPICM	Dual Purpose Improved Conventional Munitions
DRAMA	Dynamic Re-Addressing and Management for Army
DTLOMS	Doctrine, Training, Leader Development, Organization, Materiel, and Soldiers
EO	Electro-Optic
ESM	electronic warfare support measures
EW	Electronic Warfare
FBCB2	Force XXI Battle Command Brigade and Below System
FCS	Future Combat System
FFRDC	Federally Funded Research and Development Centers
FOPEN	Foliage Penetrating Radar
GIG	Global Information Grid
HPM	High Power Microwave
HUMINT	Human Intelligence
I2	Image Intensification
IA	Information Assurance
ICT	Integrated Concept Team
IDM-T	Information Dissemination Management -Tactical
IFV	Infantry Fighting Vehicle
IMINT	Imagery Intelligence
INFOSEC	Information Security
IPB	Intelligence Preparation of the Battlefield
IR	InfraRed
IT	Information Technology
KM	Knowledge Management

LIDAR	Laser Radar; light detection and ranging
MACOM	Major Army Command
MASINT	Measurement and Signal Intelligence
MDW	Military District of Washington
MLRS	Multiple Launch Rocket System
MOSAIC	Multifunctional On-the-Move Secure Adaptive Integrated Communications
NRO	National Reconnaissance Office
NSA	National Security Agency
O&O	Organizational and Operational
OSD	Office of the Secretary of Defense
PEO	Program Executive Officer
R&D	Research and Development
R/T	Real Time
RF	Radio Frequency
RSTA	Reconnaissance, Surveillance, and Target Acquisition
S&T	Science and Technology
SA	Situational Awareness
SAR/MTI	Synthetic Aperture Radar / Moving Target Indicator
SIGINT	Signal Intelligence
SLAD	Survivability Analysis Directorate
STO	Science and Technology Objectives
SUO-SAS	Small Unit Operations Situational Awareness System
SWWIM	Survivable Wired and Wireless Infrastructure for Military Operation
TI	Tactical Infosphere
TOR	Terms of Reference
TRADOC	Training and Doctrine Command
UAV	Unmanned Aerial Vehicles
UGS	Unattended Ground Sensors
UHF	Ultra High Frequency
WTC	World Trade Center

APPENDIX D

SUBPANEL SLIDES

Exploitation Algorithms and Assistants

- **Definition**
  - The automation tools used by the analyst to interpret images, tracks, signatures, etc. to answer commander's/warfighter's questions
- **Status**
  - Unique to DOD and Army has unique needs
  - Currently, most of the tools are information management and display related
  - Much effort, little demonstrated success on ATR(e.g. DARPA)
  - GMTI successful at locating and tracking ground moving targets
  - Most efforts exploit the product of a single sensor
  - Few small disjointed efforts (CECOM, ARL, DOE Labs)
- **Recommendations**
  - Plan and fund program to provide essential capabilities in collaboration with other services and agencies
  - Demonstrate in ATD's, ACTD's and tests involving Objective Force

Real Time In Cockpit

- **Definition**
  - Provides real time "heads up" display of tactical situation based on external sources
- **Status**
  - Most of required capability unique to DOD
  - Air Force and DARPA have demonstrated the capability with respect to tracking information on targets in Kosovo
    - Depends on good communications from sensor through processing to the cockpit
    - Builds on "heads up" display in modern AF aircraft
  - Did not identify any technology efforts in the Army during this study
- **Recommendation**
  - Demonstrate Army utility in an ATD by adapting Air Force/DARPA systems
  - Develop supporting technologies that prove high payoff

Visualization and Presentation

- **Definition**
  - The collection of hardware and software that "outputs" from the information systems to the human user
- **Status**
  - Rapidly evolving commercially developed technology
  - Entertainment industry moving this from the "computer driven" systems to the "human driven" systems
  - Commercial GIS systems provide much of Army's capability
    - NIMA/Army data not yet compatible with commercial standards
  - Army has exciting program with USC affiliated ISI
- **Recommendations**
  - Expand the existing Army/ISI research to include support of the Objective Force
  - Demonstrate new capabilities in ATD's

KNOWLEDGE MANAGEMENT PANEL

INFORMATION SOURCES: SENSORS and PROCESS

GARY GLASER
PAUL TILSON
ED REEDY

THE QUESTION'S

OBJECTIVE: ABILITY TO SEE FIRST, TARGET AND SHOOT

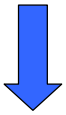
- **What observables will be available to Objective Force Operations that will provide for INFORMATION DOMINANCE?**
- **What mix of sensor systems will provide for rapidly processed data that can enable decision focused information / knowledge?**
- **What sensor systems are currently available and applicable to this objective?**
- **What sensor systems are available but require engineering redesign?**
- **What technologies need advancement to provide for necessary sensor systems for operational usage in 2008 / 2012 time frame?**
- **What knowledge management processes/system's are required to manage information flow to the user?**

41

SENSOR – DECIDER – SHOOTER CONCEPT

- **TODAY: Sensor –to-shooter functions are partitioned by function and/or echelon.**
  - **e.g., forward observer – fire direction center – battery**
- **Future sensor-decider-shooter functions will be controlled by the fighting unit and may be partitioned geo-spatially.**
- **Decider function entails complex tasks.**
  - **Sensor choice, deployment, interpretation, integration.**
  - **Rules of Engagement interpretation, application.**
  - **Target detection, identification, selection.**
  - **Weapons mix, direction, engagement.**
  - **Assess effect and re-engage.**

… and it must get done in less time at lower levels

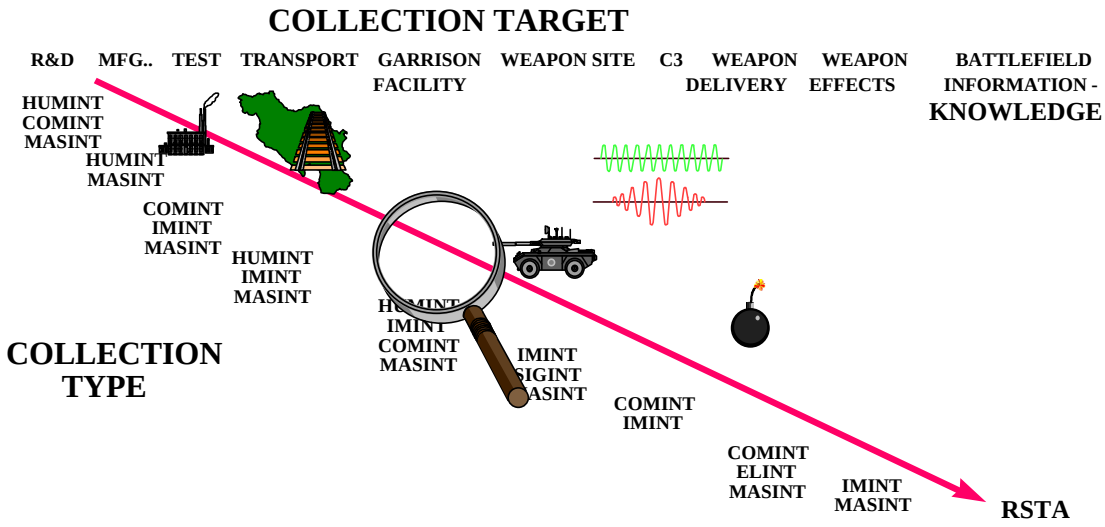


REQUIRES

KNOWLEDGE MANAGEMENT

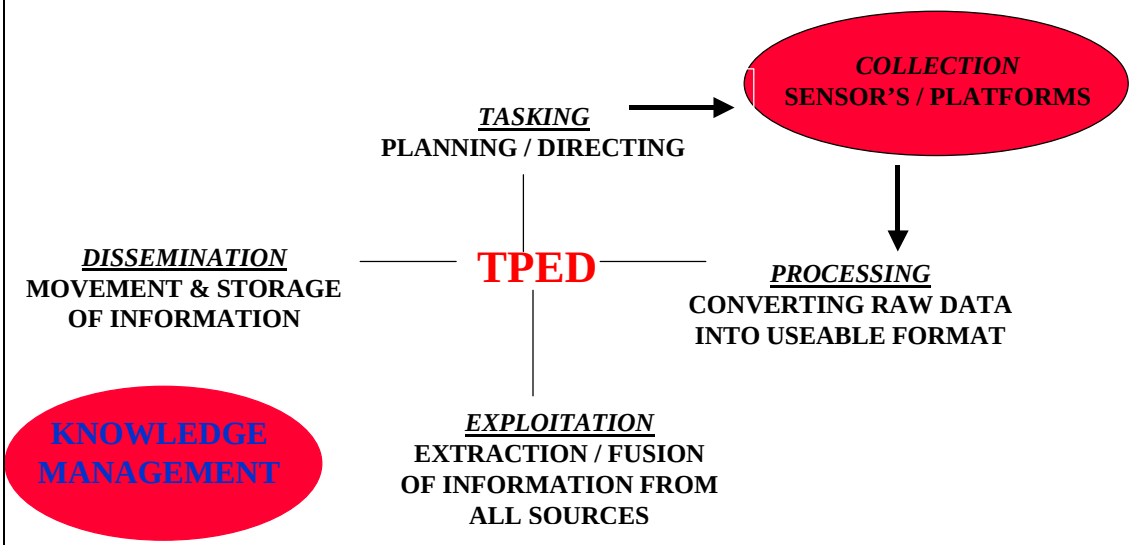
42

INTELLIGENCE, SURVEILLANCE, RECONNAISSANCE, TARGETING (ISRT)



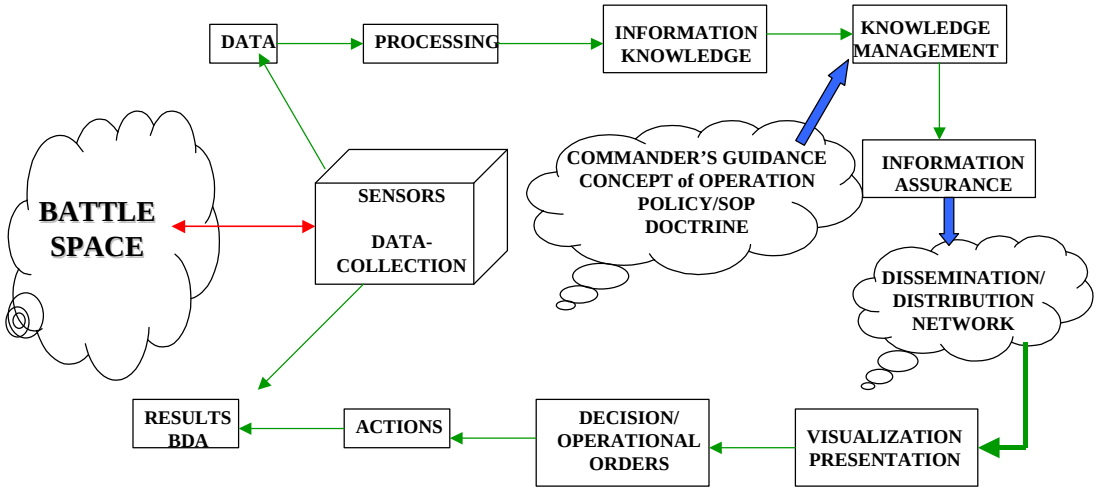
LONG TIME FRAME	WEEKS TO DAYS	WEEKS TO DAYS TO HOURS	DAYS TO HOURS	DAYS TO HOURS TO MINUTES	HOURS TO MINUTES	HOURS	MINUTES TO SECONDS

TASKING, PROCESSING, EXPLOITATION, DISSEMINATION (TPED) PROCESS

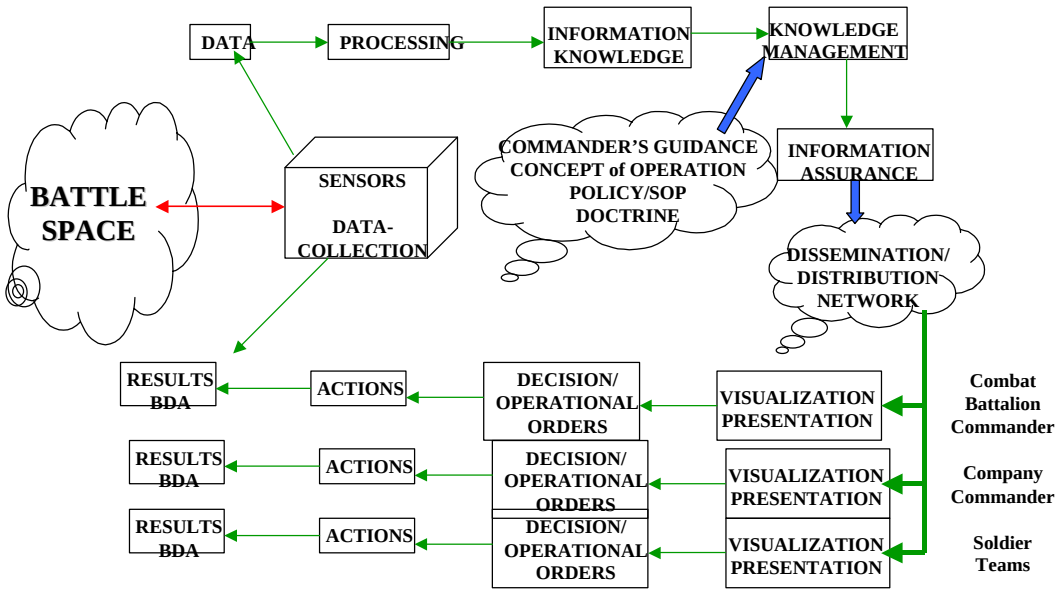


TPED PROCESS: MANAGE DYNAMIC, HIGH VELOCITY INFOMATION

BATTLEFIELD DECION MAKING PROCESS (BATTLEFIELD KNOWLEDGE MANAGEMENT)



BATTLEFIELD DECION MAKING PROCESS (BATTLEFIELD KNOWLEDGE MANAGEMENT)



THE COLLECTION WORLD

INFORMATION TYPE

- ELECTRONIC EMISSIONS
- COMMUNICATION INTERCEPTS
- IMAGES (active/passive)
- Non- IMAGED SIGNATURES (MASINT)
- HUMINT

OBSERVABLES

TYPE
- EMISSIVE
- REFLECTIVE
- TRANSMITTED
- STATIC
- DYNAMIC
- PATTERNS

COLLECTION MEANS

- ELECTRO-MAGNETIC (passive/active)
- ELECTRO-OPTICAL (passive/active)
- THERMAL (image/non-image)
- VISUAL (human)
- ACOUSTICAL

ENVIRONMENT

- WEATHER
- TOPOLOGY
- TERRAIN
- URBAN / RURAL

INFORMATION DENIAL

- CAMOUFLAGE
- CONCEALMENT
- DECEPTION

47

COMBAT BATTALION INFORMATION REQUIREMENTS

INFORMATION/OBSERVABLES	SOURCE/SENSOR	REFRESH TIME	BANDWIDTH
- ENEMY SITUATION - location/movement - composition/strength - assets/weapons - order of battle	- CONTACT REPORTS (MASINT) - RSTA ASSETS - UGS - night vision/EO - SAR/MTI radar - GSR (PPS-5); MPQ-36/37 - UAV - JSTARS ----- CGS - NTM's	Ranges from seconds	
- INTELLIGENCE	- INTELLIGENCE ASSETS - Guardrail - COMINT - SIGINT - ELINT - ASAS - GBCS - BCIS-------ATR	To hours	
- FRIENDLY SITUATION - location/movement - composition/strength - assets/weapons/status - operational plan - RSTA assets - communications - fire support	- GPS/EPRLS - SINCGARS/MTDR - STATUS REPORTS	To days	
- LOGISTICS - CONCEPT of OPERATIONS	- LOGISTICS STATUS - OPERATIONS ORDER	Depending on	
- TERRAIN	- DIGIAL TERRAIN DATA BASE - DIGITAL MAPS	Contact with enemy.	
- WEATHER	- DOPPLER WEATHER RADAR - SATELLITE IMAGERY - MET UNITS/COMPUTER PREDICTIONS		

FINDINGS

TIMELY, SUFFICIENT KNOWLEDGE Rather Than PERFECT, LATE INFOMATION

CURRENT PROBLEM: Existing single sensor, stand-alone product development rather than a total Battlefield awareness solution which inhibits plug and play and effective data exploitation ⇒ KNOWLEDGE

CORE CAPABILITY	TECHNOLOGY	PROJECTED STATUS @FY2006*	
		Technology	Programmatics
Information Management	Intelligent Data Management	Green	Yellow
	Common Operating Picture	Yellow	Yellow
	Human Machine Interface	Yellow	Red
RSTA & INTELLIGENCE	EO, IR, Radar, RF, LIDAR Sensor's	Green	Yellow
	Micro-acoustic, Seismic Sensor's	Green	Yellow
	Sensor Fusion – Deconflict, Template	Green	Red
	Multi-sensor Fusion	Red	Red
	ATR-Detection & Recognition	Yellow	Red

SYSTEM'S SOLUTION: A system's view must be taken in developing the ISRTA support architecture and products to enable the Objective Force and the associated Individual Soldier's accomplish their defined missions.
Automated situation awareness; Targeting; Ordnance awareness.
Knowledge providing "instant" detection and location of threats.
Mix of sensors – RF location; UHF radar; SAR/MTI radar; night vision; …..
Challenges – FOPEN; urban surveillance; mine detection; sensor fusion.

*** From FY2000 Army Science Board Summer Study: ISRT Panel**

Information Assurance

Dale Wagner
Judy Pinsky

25 April 2001

Objectives and Scope

- Objectives
  - Define Information Assurance (IA)
  - Identify Information Assurance Security Principles
  - Identify DoD IA Vision, Goal, and Objectives
  - Relate importance of Information Assurance to the ToR
  - Identify Key IA Challenges
  - Define Defense-in-Depth Strategy
  - Identify Key Defense-in-Depth Concerns
  - Define NSA's Role for IA
- Scope
  - Echelon: Battalion and Below
  - Timeframe: 2002 - 2008

Definition: Information Assurance (IA)

- **Information operations that protect and defend information and information systems by ensuring their**
  - **availability**
  - **integrity**
  - **authentication**
  - **confidentiality**
  - **non-repudiation**
- **This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.**

52

IA relies on a risk-management blend of managerial, procedural, and technical activities that work toward assured availability, integrity, authenticity, confidentiality and non-repudiation of information services, while providing the means to efficiently reconstitute these vital services following an attack. Information Assurance is comprised of several security principles. They are Confidentiality, Integrity, Authentication, Non-repudiation and Availability. They are defined as follows:

IA Security Principles

- **Availability - Timely, reliable access to data and services for authorized users**
- **Integrity - Protection against unauthorized or destruction of information**
- **Identification and Authentication - Security measure designed to verify an individual's authorization to receive specific categories of information**

Availability - Timely, reliable access to data and services for authorized users.

Integrity - Protection against unauthorized or destruction of information.

Identification and Authentication (I&A) - A Security measure designed to establish the identity of the sender of the message and the validity of the transmission, message, or originator, or a means of verifying an individual's authorization to receive special categories of information.

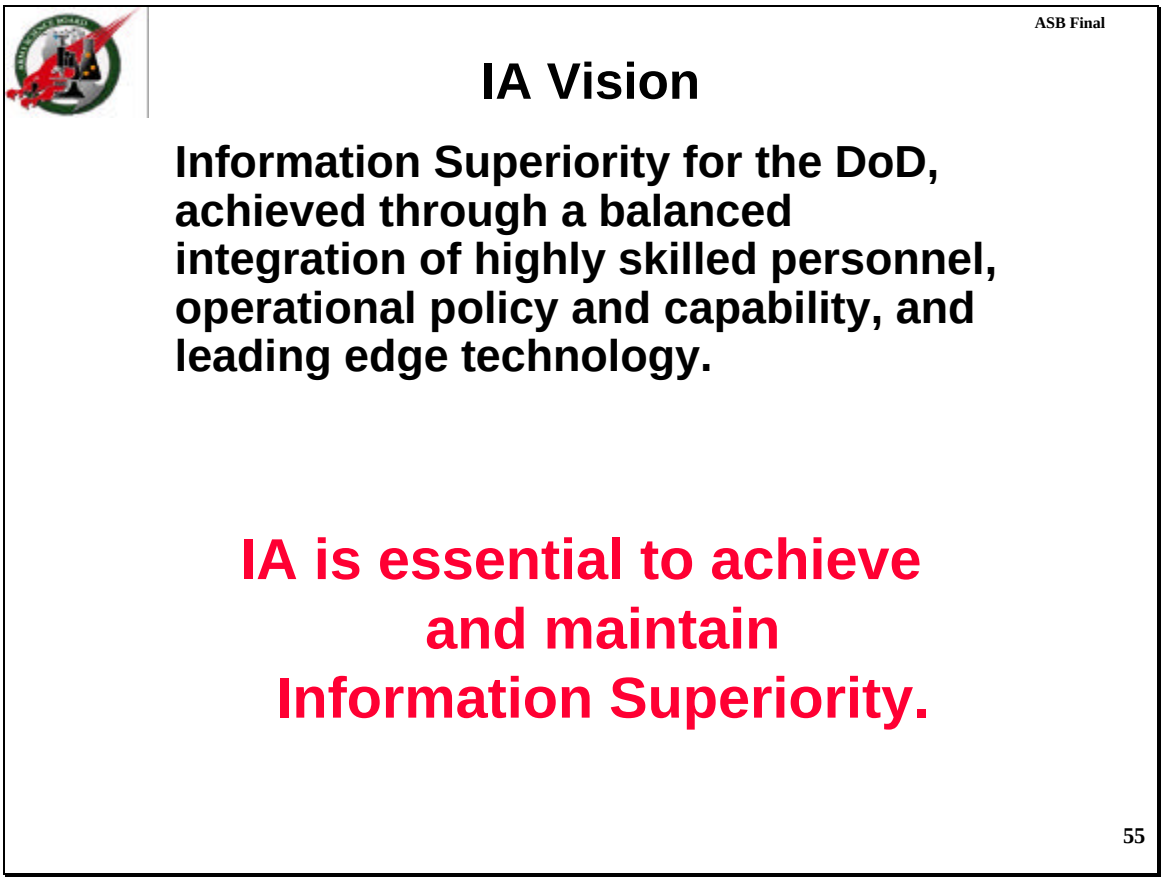
IA Security Principles (con't)

- **Confidentiality - Assurance that information is not disclosed to unauthorized entities or processes.**

- **Non-repudiation - Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.**

Confidentiality - Assurance that information is not disclosed to unauthorized entities or processes.

Non-repudiation - Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.



Joint Vision 2020 presents both operational concepts and challenges to the Warfighter to counter the asymmetrical threat of Information Operations in order to achieve Full Spectrum Dominance in the electronic battlefield.

The Department of Defense has begun deploying a layered strategy to protect its Information Technology (IT) environment and detect and respond to cyber threats through Information Assurance mechanisms utilizing a Defense-in-Depth approach. The Army has adopted this defense in depth approach. The defense in depth concept is applicable for the Combat Battalion's Knowledge Management system.

IA Goal

Ensure DoD's vital information resources are secure and protected.

IA Objectives

- **Make IA an integral part of DoD mission readiness criteria**
- **Enhance DoD personnel information assurance awareness and capabilities**
- **Enhance DoD IA operational capabilities**
- **Establish an integrated DoD security management infrastructure**

Information Assurance and the ToR (1 of 2)

- **"Information Dominance…" is dependent upon:**
  - **providing reliable access to the right information at the right time**
  - **insuring the accuracy and relevance of needed information**
- **"…define information assurance..." is based on the need to:**
  - **protect information that impacts national security**
  - **authenticate sender and intended receiver**
  - **minimize the risk of cyber attack and the lost of confidentiality**

Information Assurance and the ToR (2 of 2)

- **"...imperative that our Forces have the adequate information assurance technologies…" involves the integration of:**
  - **a Defense in Depth approach applicable for the Combat Battalion's Knowledge Management System**
  - **appropriate NSTISSP evaluated and validated security products and services**

Information Assurance Challenges

- Interconnected, interdependent systems underscore need for broad understanding of threats and vulnerabilities
- Security-enabled commercial products - strong encryption with key recovery (Except for Digital Signature)
- Global Security Management Infrastructure
- Cyber situation awareness - Cyber attack, sensing, warning and response capability

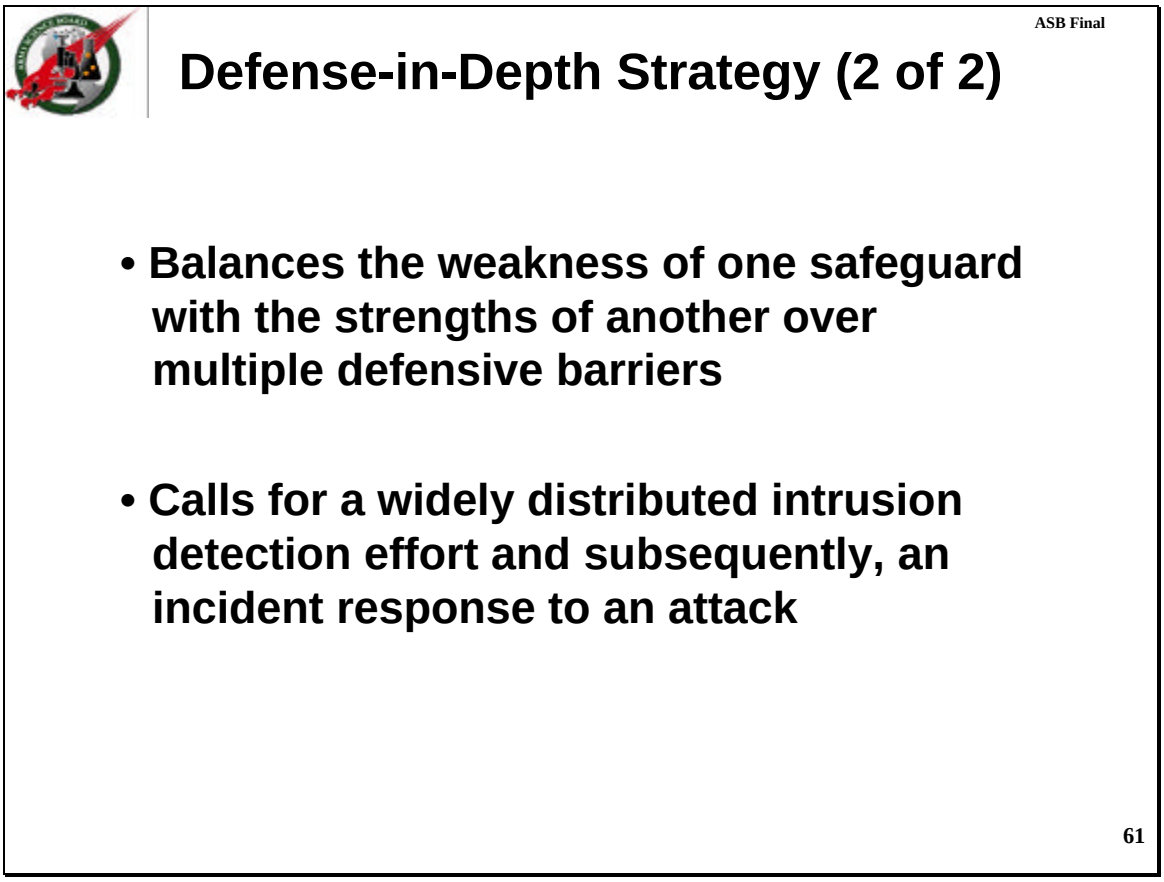
Defense-in-Depth Strategy (1 of 2)

- **Provides an active cyber defense capability**
- **Integrates the Operations, Technology, and Personnel capabilities to establish protection across multiple layers and dimensions**
- **Helps create an information environment where adversaries will face successive layers of defense**

1. The Defense-in-Depth strategy for IA provides capability, which is based on the ability to protect information and information systems, detect and report intrusions in information systems, and respond to these attempted intrusions.

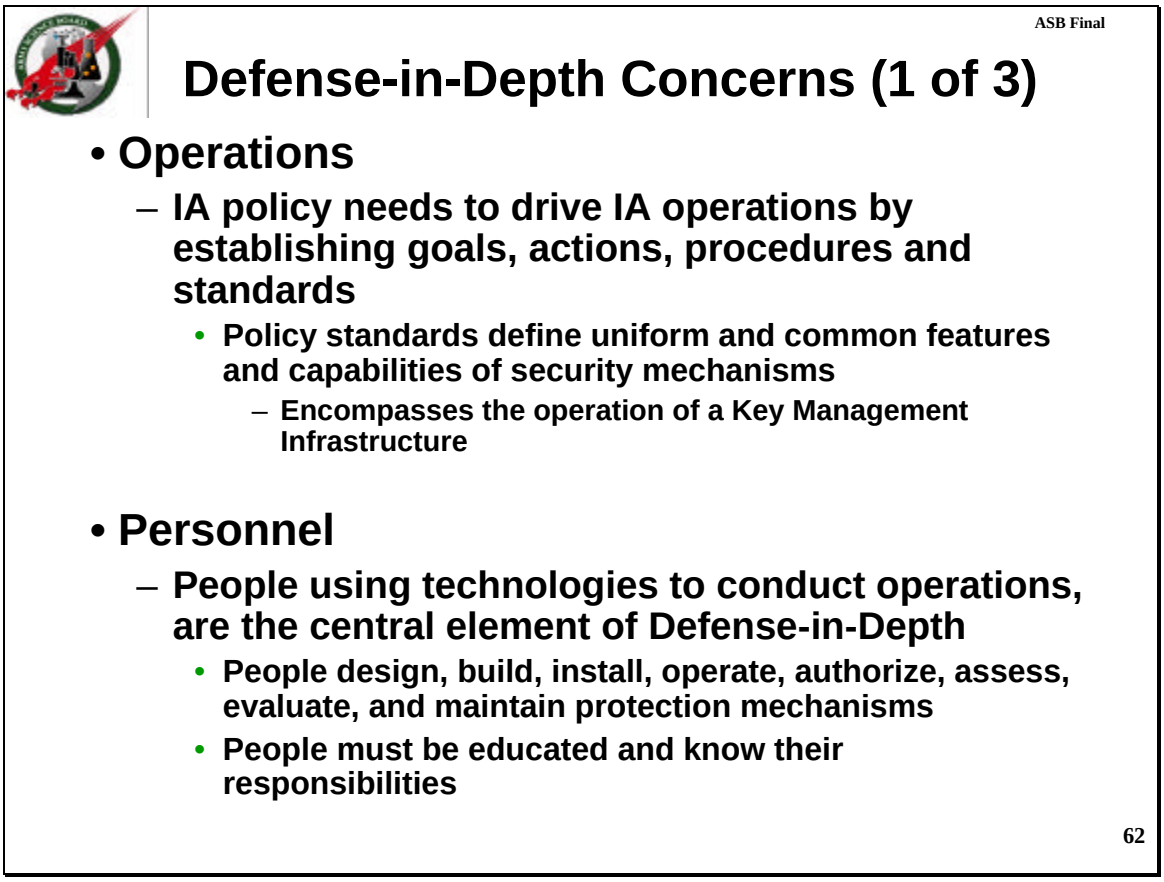
2. The strategy integrates the Operations, Technology, and Personnel capabilities to establish protection across multiple layers and dimensions--analogous to the defenses of a castle.

3. Defense-in-Depth helps create an information environment where adversaries will face successive layers of defense, each of which employs a variety of security methods.



4. This strategy balances the weakness of one safeguard with the strengths of another over multiple defensive barriers.

5. The strategy also calls for a widely distributed intrusion detection effort and subsequently, an incident response to an attack.



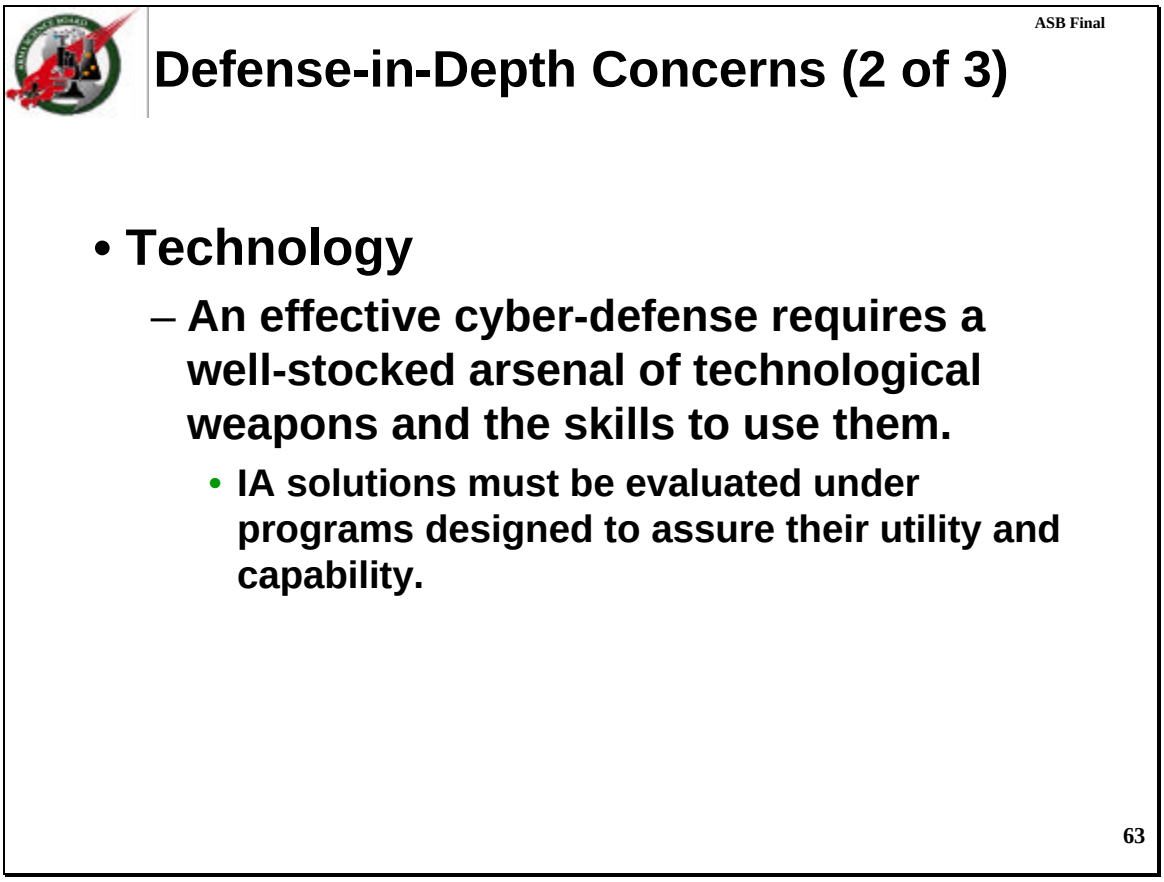
A Defense in Depth (DiD) Initiative is dependent upon:

Operations

IA policy drives IA operations by establishing goals, actions, procedures, and standards. IA policy formally states the security requirements in terms of what must be done and not done. Policy establishes standards that define uniform and common features and capabilities of security mechanisms, the rule or basis by which to measure the various dimensions of IA, and the desired or required level of attainment. This encompasses the operation of the Key Management Infrastructure and the operation of a layered, integrated Attack, Sensing, Warning and cyber situation awareness and analysis capability with coordinated response mechanisms.

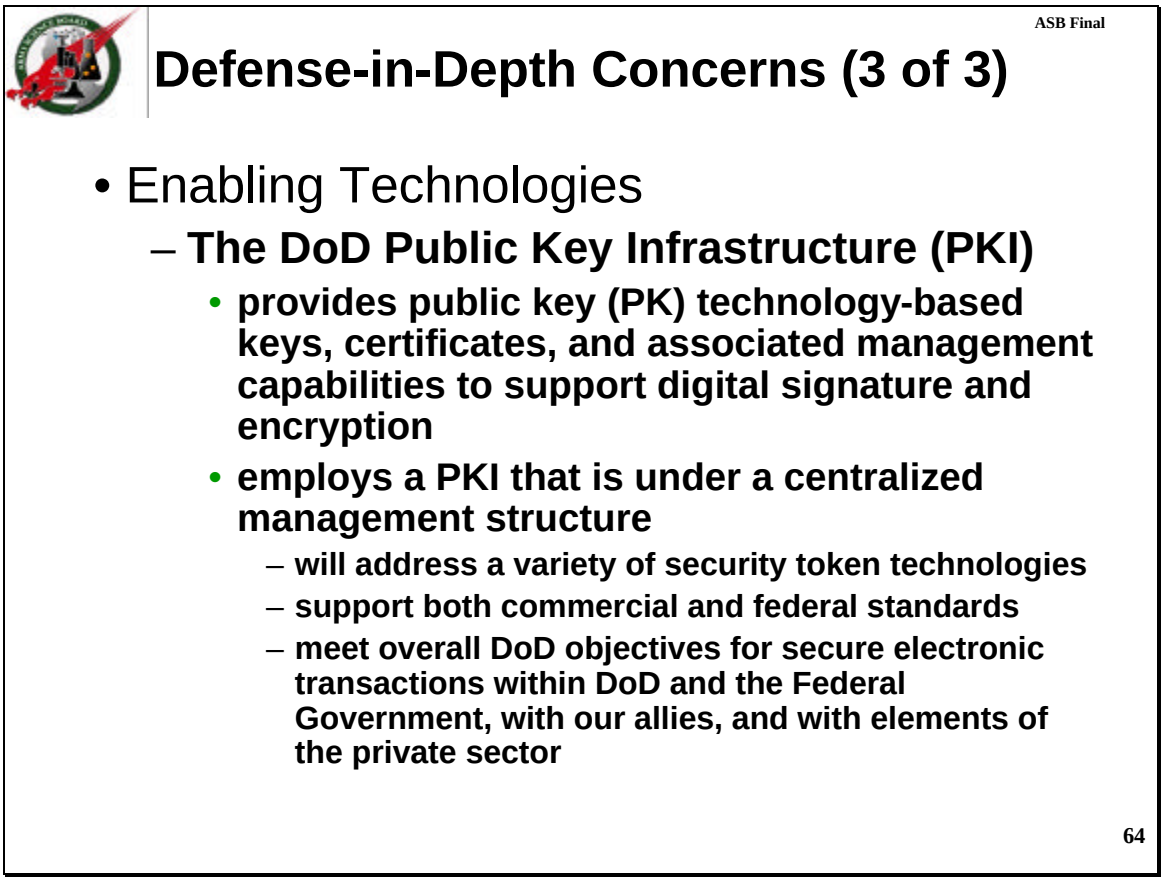
Personnel

People, using technologies to conduct operations, are the central element of DiD. People design, build, install, operate, authorize, assess, evaluate, and maintain protection mechanisms. People must also be educated and made aware of their responsibilities within the DiD architecture.



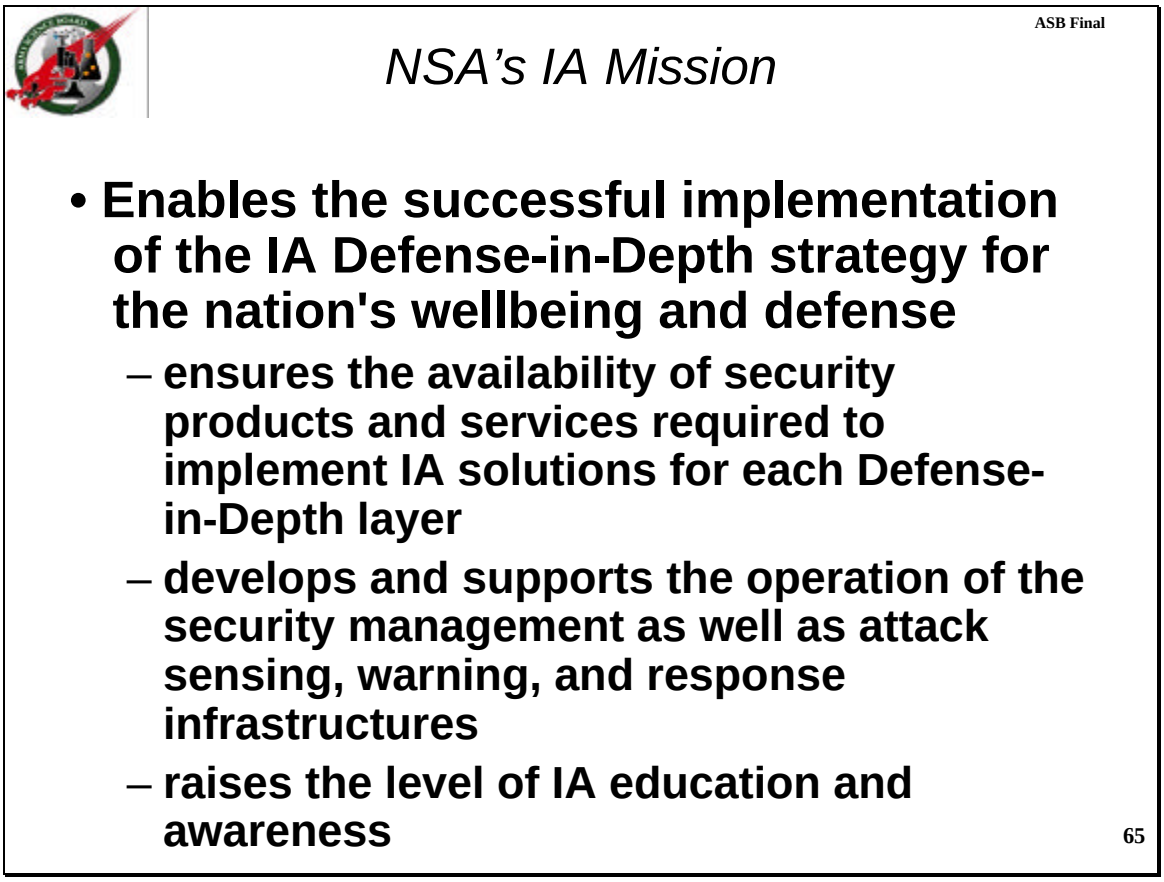
Technology

To conduct an effective cyber-defense, DoD must have a well-stocked arsenal of technological weapons and the skills to use them. DoD has greater confidence in the effectiveness of the technology tools and products used in DoD IA solutions because they must be evaluated under programs designed to assure their utility and capability.



Enabling Technologies

The DoD Public Key Infrastructure (PKI) enables the IA security services of data integrity, user-identification and authentication, user non-repudiation, and data confidentiality for electronic information interchange. This is accomplished by providing the public key (PK) technology-based keys, certificates, and associated management capabilities to support digital signature and encryption. These PK-enabled IA services and applications provide for the protection of transactions from unauthorized data disclosure and modification, and provide positive access control to system resources. To ensure interoperability among DoD users and to minimize operational costs, DoD will employ a PKI that is under a centralized management structure, yet will support outsourcing and distributed Service/Agency operation of some of the PKI components. The integrated enterprise-wide PKI will address a variety of security token technologies, support both commercial and federal standards, and meet overall DoD objectives for secure electronic transactions within DoD and the Federal Government, with our allies, and with elements of the private sector.



NSA's IA Mission

The main trust of NSA's Information Assurance (IA) mission is to enable the successful implementation of the IA Defense-in-Depth strategy for the nation's well being and defense. Enabling Defense-in-Depth for the Nation ensures the availability of security products and services required to implement IA solutions for each Defense-in-Depth layer; develops and supports the operation of the security management as well as attack sensing, warning, and response infrastructures; and raises the level of IA education and awareness.

NSA's IA Objectives (1 of 2)

- **Provide the products, services, infrastructure, and capability necessary to assure the availability and appropriate application of NSTISSP evaluated/validated security products/solutions to satisfy the technology objectives for each Defense-in-Depth layer.**

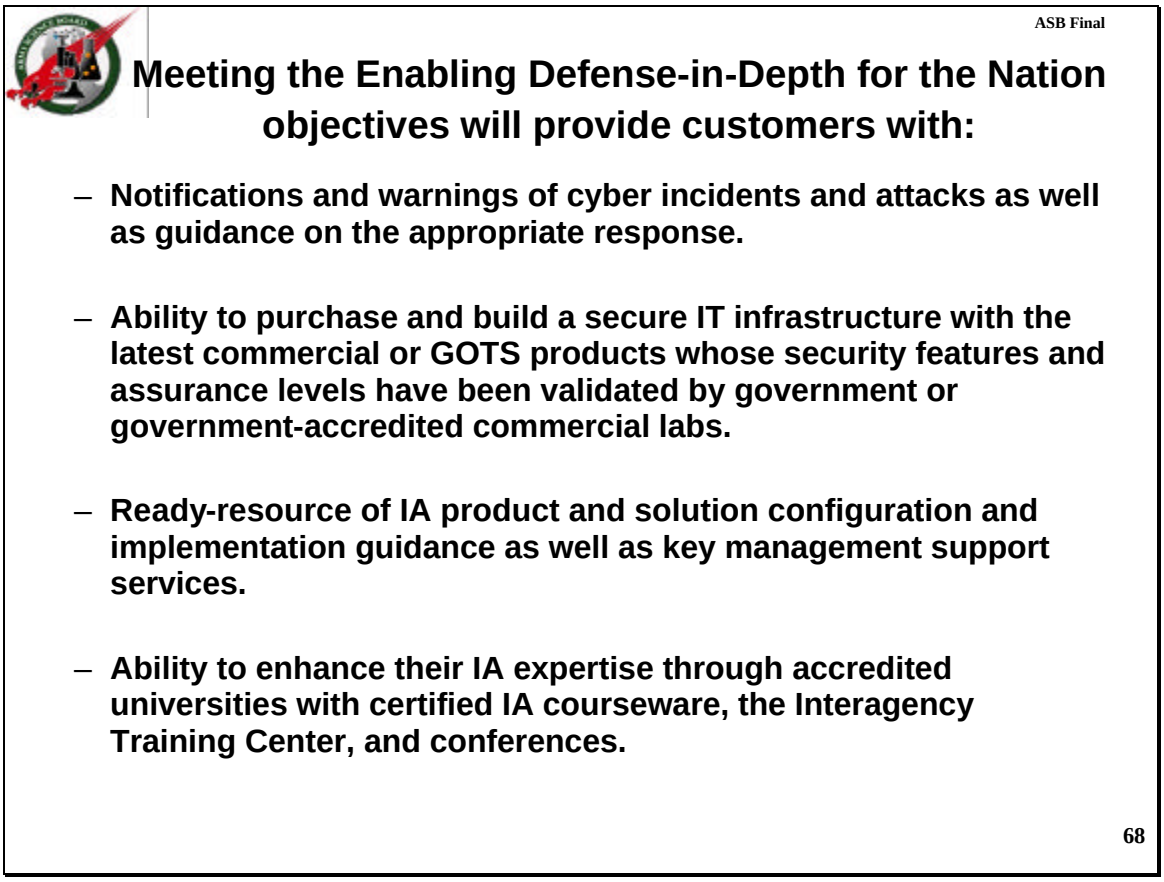
- **Conduct Defensive Information Operations (DIO) in partnership with CINCSPACE , the Director of the joint Task Force-Computer Network Defense (CND) and the Defense Information Systems Agency.**

DIO ensure the timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and systems.

Computer Network Defense (CND) is a subset of IA protection activity, consisting of actions taken pursuant to legal authority to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.

NSA's IA Objectives (2 of 2)

- **Provide Key Management and Public Key Operations for the National Security Command.**
- **Increase national IA education and awareness.**



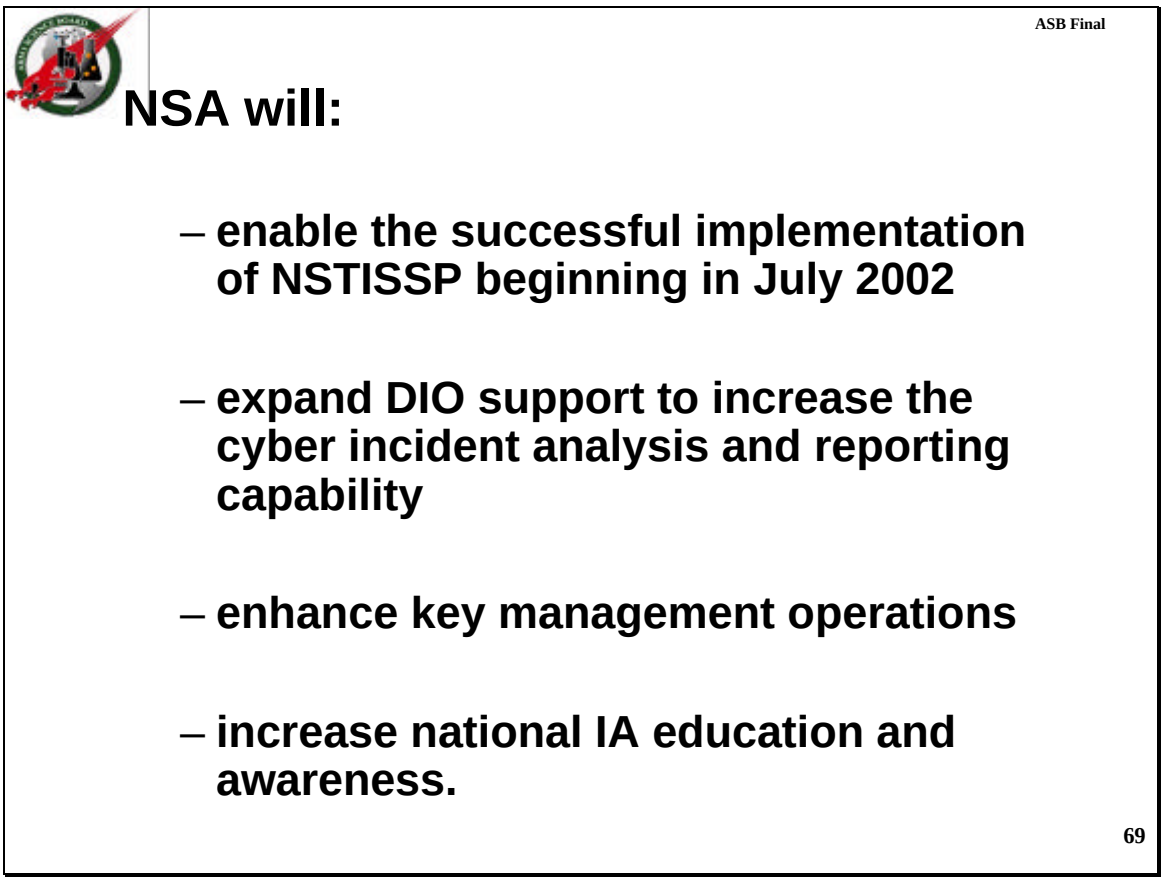
Meeting the Enabling Defense-in-Depth for the Nation objectives will provide customers with:

Notifications and warnings of cyber incidents and attacks as well as guidance on the appropriate response.

The ability to purchase and build a secure IT infrastructure with the latest commercial or GOTS products--products whose security features and assurance levels have been validated by government or government-accredited commercial labs.

A ready-resource of IA product and solution configuration and implementation guidance as well as key management support services.

The ability to enhance their IA expertise through accredited universities with certified IA courseware, the Interagency Training Center, and conferences.



While NSA's resources and activities primarily focus on the successful implementation of the Defense-in-Depth strategy within the National Security Community, they are leveraged through partnerships with government, industry, and academia to benefit the national IT infrastructure.

Information Exploitation

Lynn Gref
William Howard III

24 April 2001

Definition: Information Exploitation

- **In ISR context, information exploitation refers to the interpretation of images, tracks, signatures, etc. to answer the questions of who, what, where, when, how and intent.**

Information Exploitation Functions

- Provides the IPB (Intelligence Preparation of the Battlefield)
  - Terrain
  - Location and activities of enemy units
  - Location and activities of neutrals and non-combatants
  - Location and characteristics of potential targets
- Identifies possible intent of opposing commander including threat assessments
- Provides attack warning
- Provides damage assessment

Information Exploitation and the ToR

- "… conquering the information glut …" is dependent on information exploitation to
  - Reduce the "passing along data" for interpretation by the warfighter and the decision maker
  - Answer questions rather than confuse the issue with irrelevant information
  - Reduce the "fog of war" through the elimination of redundant, irrelevant, contradictory, untimely, meaningless data or information
- "… mitigate asymmetric threats …" is dependent on information exploitation to
  - Provide the knowledge base on which to shape the course of action and protect our forces.

Selected Information Exploitation Issues

- Currently, exploitation is human resource and infrastructure intense (e.g. image or signal analysis)
- Capabilities needed
  - Analysts' automation assistants and filters
  - Integrated multi-sensor exploitation (e.g. "field" of seismic sensors)
  - Multi-source exploitation (e.g. SAR, GMTI, imagery, and seismic)
  - Integrated "single picture" presentation including terrain
  - Standardized reliable products and presentations
  - All source exploitation strategy (e.g. terrain and IPB from national means, unit tracks and broad area coverage from theater means, specific situational awareness from organic sensors)
- Coping with constraints
  - Incomplete and/or non-resolvable information
  - Required timelines and infrastructure limitations

Selected Assumptions

- The USA will employ the following philosophy with respect to Information Exploitation
  - Utilize an analyst based approach that is supported by a capable infrastructure including maximum support from automated aids.
  - Recognize its uniqueness to the DoD and thereby develop it in concert with other Services and Agencies
  - Adopt a multi-tier solution which performs exploitation as far from combatants as possible
- Information Exploitation receives the attention and funding necessary to support the Objective Force
- Information Exploitation will be balanced with collection and distribution systems

Concerns (1 of 2)

- In order to enable effective tactical Knowledge Management, careful consideration must be paid to the following exploitation issues
  - A cohesive systems approach must be taken
  - The “holy grail” of automated target recognition and fully automated information exploitation must be avoided
  - “Just-in-time” and “good enough” approaches need to be identified and pursued
  - Study assumptions must become reality
  - Needed capabilities must be developed that satisfy the constraints

Concerns (2 of 2)

- DARPA, other Services and the Laboratories have important capabilities and promising efforts underway that need to be incorporated into the Army’s solution
- Georectification of geospatial data vital to information exploitation depends on GPS which is fragile until the deployment of GPS III
- Effective information exploitation is mutually dependent the appropriate suite of collection and management systems.

Key Opportunities for Improvement

- Real exploitation of multi-source information
- Automation aids for the analyst, the commander and the warfighter
  - Recognize they will be essential to the objective force
  - Assist in "change detection"
  - Creating a standardized presentation format
  - "Data filters"
- Sensor "tasking" based on information exploitation needs
- Exploitation of non-organic sensors
  - Improve effectiveness and utility of organic sensors

Observations

- In order to enable effective tactical Knowledge Management, it is vital that enhancements be made in
  - Use of all potential sources of information
  - Analysts' automation aids and filters
- Information exploitation is a tough problem and requires solutions to many individual problems
- Information exploitation will require human analysts supported by a large infrastructure for the foreseeable future
- Inadequate resources have been programmed to develop and acquire the needed information exploitation capabilities

Exploitation Algorithms and Assistants

- Definition
  - The automation tools used by the analyst to interpret images, tracks, signatures, etc. to answer commander's/warfighter's questions
- Status
  - Unique to DOD and Army has unique needs
  - Currently, most of the tools are information management and display related
  - Much effort with little demonstrated success on ATR (e.g. DARPA)
  - GMTI successful at locating and tracking ground moving targets
  - Most efforts on exploitation of the product of a single sensor
  - Few small disjointed efforts (CECOM, ARL, DOE Labs)
- Recommendations
  - Plan and fund program to provide essential capabilities in collaboration with other services and agencies.
  - Demonstrate in ATD's, ACTD's and tests involving Objective Force

Real Time In Cockpit

- Definition
  - Provides real time "heads up" display of tactical situation based on external sources
- Status
  - Most of required capability unique to DOD
  - Air Force and DARPA have demonstrated the capability with respect to tracking information on targets in Kosovo
    - Depends on good communications from sensor through processing to the cockpit
    - Builds on "heads up" display in modern AF aircraft
  - Did not identify any technology efforts in the Army during this study
- Recommendation
  - Demonstrate Army utility in an ATD by adapting Air Force/DARPA systems
  - Develop supporting technologies that prove to have high payoff

Visualization and Presentation

- **Definition**
  - The collection of hardware and software that "outputs" from the information systems to the human user
- **Status**
  - Rapidly evolving commercially developed technology
  - Entertainment industry moving this from the "computer driven" systems to the "human driven" systems
  - Commercial GIS systems provide much of Army's capability
    - NIMA/Army data not yet compatible with commercial standards
  - Army has exciting program with USC affiliated ISI
- **Recommendations**
  - Expand the existing Army/ISI research to include support of the Objective Force
  - Demonstrate new capabilities in ATD's

Synchronized Secure Distributed Database

- **Effective and accurate dissemination of a knowledge will rely on some type of synchronized and secure distributed database system.**
  - Database must be consistent so queries answered from different sources are the same.
  - Databases must be synchronized so information stored at different sites is consistent.
  - Database must be secure so unauthorized access does not corrupt the system.

- **Technologies will need to be addressed by both commercial and the Department of Defense to ensure database integrity.**
  - Multiple rules sets for data integration.
  - Improved system management so administrative overhead does not strangle the network

A distributed database system is defined as a collection of multiple, logically interrelated databases distributed over a computer network. There is a strong distinction between a distributed database system, and a centralized database system where the data is stored at several locations.

In a distributed database system, each site maintains part of the database, and the site has autonomous control over its data. Thus, parts of the database are maintained at different locations where communication occurs over a network. Since each site handles a portion of the database, an advantage of a distributed database system is that processing times and input output services are faster for users accessing data from their local database. However, the disadvantage is that network queries across the system could over-burden and deadlock the network. Since data is replicated in a distributed database, it exists at more than one site, thus a disturbance or outage at one site will not effect other locations. However, the disadvantage is that distribution of the data creates problems of synchronization coordination and integrity. Data in a distributed database system must be consistent, meaning differences in identical data fields that are stored at different locations must be found, and correctly fixed. Security in any database system may be broken down into two components: data protection and authorization control. However, in a distributed database system, additional opportunities for denial of service attacks may exist due to the communications required to synchronize the different parts of the database.

Briefings to the Army Science Board from Oracle Corporation and Mitre indicate there is no near term solution to the problems associated with synchronization and consistency in distributed databases. The commercial sector has, and will continue to make great strides in distributed databases, however, commercial databases are located at fixed locations connected by high bandwidth communication lines. The Army distributed database problem has the additional characteristic of mobility.

Malicious Code

- **Any knowledge management system will send messages across a network, most likely employing commercial off the shelf software and hardware.**
  - Malicious code may be defined as a computer program that intentionally does harm to an information system. Popular terms for types of malicious code are: Virus, Worm, Trojan Horse and Logic Bomb.
  - Most experts agree it is impossible to completely protect information systems from malicious code. Message attachments, rogue computer programmers, and unwitting users are all entry points for malicious code.

- **There does not exist sufficient technology or research devoted to malicious code to eradicate this problem.**
  - As long as systems remain connected and individuals can download attachments or insert floppy disks there will always be an opportunity for malicious code to be inserted.
  - Additionally, software manufacturers usually do not guarantee their code is free from logic bombs.

Malicious code may be a self-contained program, but usually malicious code is hidden as part of larger software programs. Popular terms for types of malicious code are:
Virus - A computer program, which when executed, can attach itself to another program without permission or knowledge of the user.
Worm – A program that copies itself into the nodes on a network (it does not have to be transmitted by a user).
Trojan Horse – Named after the deceptive wooden horse used by the Trojan Army, a Trojan horse is a computer program that masquerades as something it is not. Note by common definition, viruses and worms replicate themselves while a Trojan horse does not.
Logic Bomb – Dormant code that is triggered by an action or event to do something that is not expected by the user.
The above types of malicious code can be combined, for example, an email attachment may appear to be a simple Word document, however, the Word document is a Trojan horse that unleashes a virus on the system. Likewise, a surreptitious computer programmer plants a logic bomb in a commercial computer program that allows the original programmer access to files controlled by the code through the use of a backdoor or secret password.
In a briefing presented to the Army Science Board Information Dominance Panel in February 2000, CECOM representatives discussed defense in depth and other measures the Army may implement to combat malicious code. However, the funding and effort spent on detecting malicious code, both commercially and in the government, is dwarfed by the opportunity for individuals to do inflict damage through the use of malicious code. As long as systems remain connected and individuals can download attachments or insert floppy disks there will always be an opportunity for malicious code to be inserted. Additionally, software manufacturers usually do not guarantee their code is free from logic bombs.

ASB Final

Next Generation Internet (NGI)

- Today's Internet not scaleable to meet demand for new missions such as national security
- Government leadership role since 1996:
  - **3 Goals: Promote Experimentation, Develop Testbed, and Demonstrate new applications to meet important national goals and priorities**
  - **Measured by quality of service, adoption of new technologies, research and application results,** 100-1000 times **end-to-end performance improvement, 100 research institutes connected, value of applications in testing network**
- Multi-agency Federal R&D NGI program created:
  - **$300M invested 1998-2000**
  - **DARPA, NSF, DOE, NASA, NIH/NLM, & NIST**
  - **More capable, powerful networks for 21st century**
  - **Form partnerships w/ industry and academia to keep U.S. on cutting edge of information and communications technologies**
  - **Introduce new network services**

85

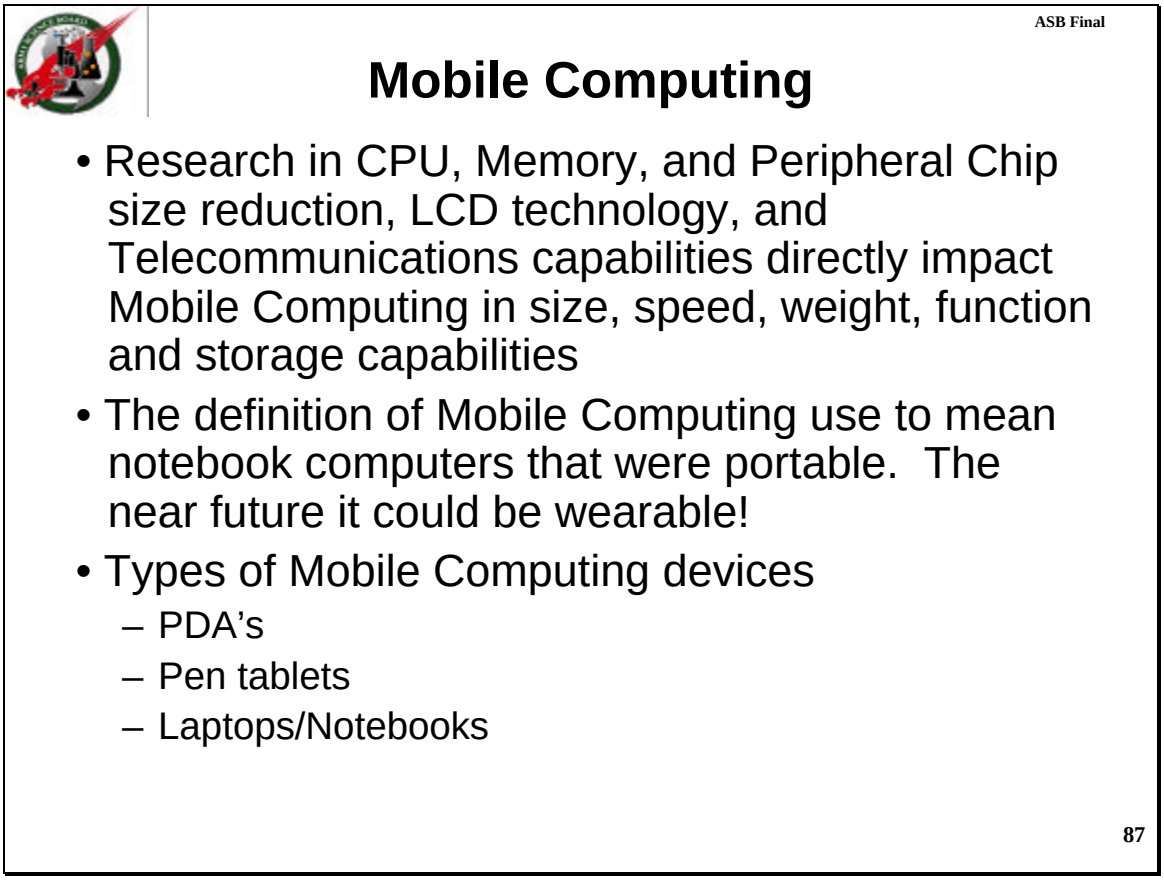
Above is based on information obtained from DARPA and presentations by Kay Howell, Director of National Coordination Office for Computing, Information, and Communications and a report entitled "Research Challenges for the Next Generation Internet, May 12-14, 1997, and by Computing Research Association, edited by Jean E. Smith & Fred W. Weingarten.
The DARPA/ITO NGI program is developing technologies that address enabling networks to scale dramatically in size, speed, and reach, focusing particularly on the capability to robustly accommodate extreme ranges of user demand:
Large bandwidth on demand across various medium (Twisted Pair, Fiber, Satellite, Wireless) (OC-768 [40Gbps] or higher in the near future!?)
Managing and analyzing networks as they grow in complexity (CAIDA)
Established a wide area research test bed called the SuperNet that spans across the country with capabilities of OC48 (2.5Gbps) data rates and regional OC192 (10Gbps) data rates over fiber optic links. (NTON, HPCC, ONRAMP, BossNet, ATDNet/MONET)
Develop applications that can handle gigabit data rates, just to name a few:
Remote Radar Control (CSU/CHILL)
HDTV over the SuperNet (ATDNEt/MONET)
Multicasting of video and audio over the net in real time (Digital Amphitheater)
Remote access of large scale database storage and retrieval systems across the SuperNet, such as Digital OrthoQuadrangle photographs w/1 Meter resolution of the Earth (Digital Earth).
Some of the enabling technology research has accelerated development of leading edge technology and has led to new startup companies and their products becoming available as COTS, such as GigaEthernet (1Gbps) routers and pc nic cards.

Implications of NGI

- Predicting the evolution of the Internet is very difficult
- NGI and other industry breakthroughs will drive the future Internet:
  - **Instant Messaging**
  - **Decentralized post-client-server Peer-two-Peer (P2P) Infrastructure and communications**
- P2P may mark fundamental change in architecture
- Control and security dimensions could be staggering
- DoD & Army Combat Research Programs rely on COTS solutions, technologies, and infrastructure
- Cross-sharing and careful targeting of research programs and good customer behavior is crucial to success

Internet evolution will likely occur in breakthrough increments driven by industry's investments in commercial-off-the-shelf products. The growth of "instant messagaing" and decentralized, post-client-server P-2-P infrastructure and communications (essentially individuals talking with each other and sharing files without going through a central control point.) According to Dick O'Neill of the Highlands Form, four factors distinguish this emerging mode:
(1) it is inherently flexible, because every node is also a control point; each user can have his or her unique experience and organizational structure, because the application logic resides in a user's peer client rather than a central server for many users;
(2) these configurations may be much more scalable, because if designed well they take advantage of self-organization;
(3) they leverage the underutilized power of networked PC's; and
(4) they are hard to control.
This holds extraordinary promise not just for sharing music files, as Napster does, but it takes advantage of the Internet as opposed to the Web to bring people and files and computing power together in loose, large configurations that are difficult to spot, pin down, and control.
Just as the potential power and use of the p-2-p infrastructure are large, the security dimensions could be staggering. Peer to Peer networking may mark a fundamental shift in the architecture, just as demand for IM (instant messaging) parallels the desire for people to go beyond the boundaries that have been established."
The transition of the NGI enabling technology and research to various DoD agency's will help achieve the future goals and objectives in the interest of national security. The necessary bandwidth to provide secure two way communications, (in the forms of audio, video, and data) between the commanders and the soldiers in the field in real time will allow for rapid resolution of the situation with all concerned.

By all parties involved being able to see, hear, and identify the battlespace, the opposition and their force strength, capabilities, and locations in the shortest period of time will allow for effective assessment and execution to nullify the problem. This will require the networking of Satellite, Wireless, Twisted Pair, and Fiber Optic mediums into a seamless environment to the end users. Management of these assets will require gigabit applications to execute, digest, and distribute the relevant information to all in real or near real time.

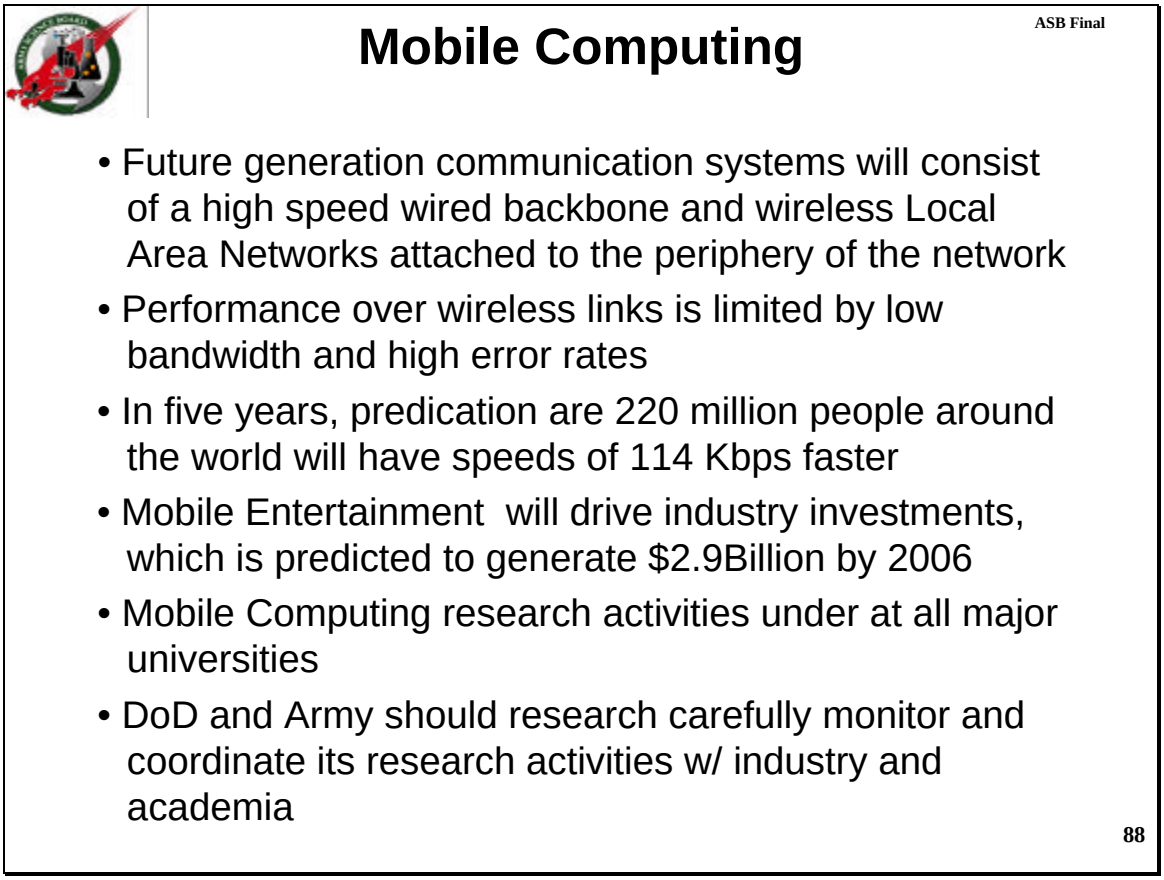


Mobile Computing hardware is getting smaller, lighter, faster, with higher resolution LCD video, longer battery life, built in microphones and speakers, and increase in the number of accessories that can be attached. The devices can be stand alone, attached to networks via 10/100 BaseT PC Ethernet cards or built-in for LAN access, internal Modem ports with speeds up to 56Kbps, InfraRed ports, wireless such as 802.11b PC cards or BlueTooth PC Cards in addition to the standard Serial, Universal Serial Bus (USB), and Parallel ports available. The storage devices can be High capacity 10-20 GB Hard Disk Drives to Memory Cards from 4MB to 64MB or more as the technology progresses.

The mobile computers can be in the form of PDA's, pen tablets, laptops, and notebooks, depending on processor power, unit size, accessories included in the unit or attached to the units. Possibilities of "Wearable" computers could be the next progressive step in mobile computing, with flexible screens and modular components communicating using BlueTooth communications technology.

Some examples of mobile computing current peripheral device data rates:
Ethernet 10/100BaseT = 10Mbps to 100Mbps MAX data throughput in ideal conditions over LANS using copper twisted pair CAT 5e, future Gigabit Ethernet or GigE (1Gbps) possible. Not many fiber optic pc cards for connectivity yet.

Standard Modems = 56Kbps dialup using RJ11 phone jacks over POTS (V.90 33.3Kbps Upload and 53Kbps Download)
IR = 750Kbps, 1.2Mbps, and 4Mbps
USB = 12 Mbps Max., but is shared as more and more USB devices are added.
i.LINK or IEEE 1394 Fire wire connections = <400Mbps
Wireless 802.11b up to 11Mbps in a LAN configuration
Wireless CDPD 128Kbps possible but most are 9.6Kbps –28.8Kbps with limited but expanding coverage by the commercial cellular providers over wide areas.
BlueTooth wireless, up to 1Mbps within a 10 meter radius.

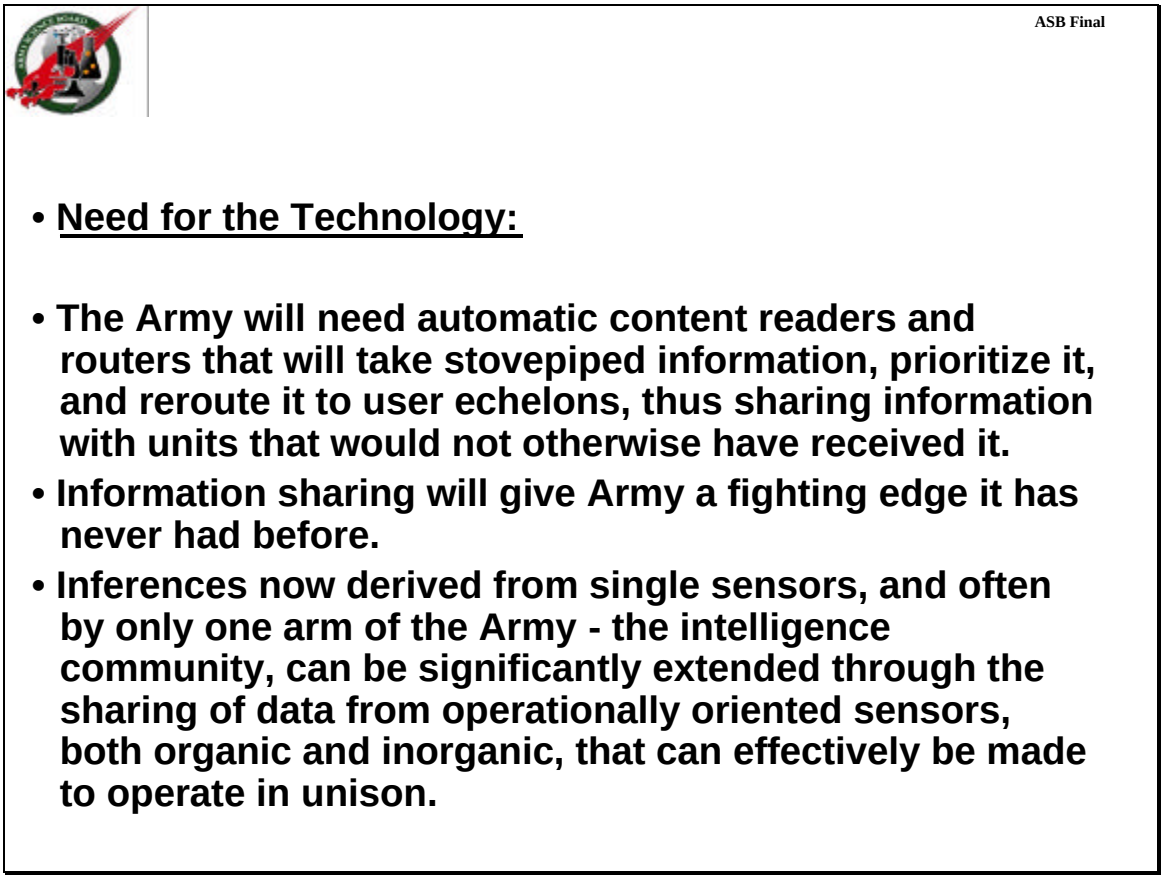


Emerging trends in technology indicate that future generation communication systems will consist of a high speed wired backbone and wireless Local Area Networks attached to the periphery of the network. Wireless LANs extend the coverage of broadband services and provide ubiquitous network access to mobile users. There are, however, many technical challenges to overcome before the vision of ubiquitous computing can be realized.
As wireless network connection speeds improve and the price of transferring data drops the public will embrace mobile entertainment, according to a new study by Webnoize. Study explained that data transfer is not possible with analog networks, a large number of which still exist in the U.S. However, digital networks have emerged that offer data rates of 9.6 or 14.4 kilobits per second (Kbps), depending on the technology the carrier is using.
In Europe, Asia and Australia, companies are working on faster connection speeds of 30 to 50 Kbps. In addition, these connections will be always on, meaning there is no need to dial-up. Other, more sophisticated networks are on the way, Bailey said, such as the much anticipated "3G," or "Third Generation" mobile communications systems. Bailey predicts wireless

connection speeds will start to increase rapidly in many parts of the world in the next 12 months. "In five years, we expect more than 220 million people around the world will have speeds of 114 Kbps faster.

Costs are expected to fall by 90 percent over the next five years," he said. "That will make it affordable for people to stream songs. In the next five years, consumers will stream both music and video on their mobile devices." More information on Webnoize is available on the Web at webnoize.com.

Extensive research underway at all major universities to investigate issues in mobile computing and multimedia to devise innovative solutions to the technical challenges in these areas. Both areas face performance limitations and require optimizations for the unique characteristics of these media. Furthermore, solutions to problems that arise when these two areas are integrated are being investigated. DoD and Army should carefully monitor and coordinate its research activities to with industry and academia to maximize returns.



- **Characteristics of the Technology:**

A "reader/router" that takes message traffic, reduces its contents, and routes it to
appropriate user elements.
- **The more automatic the process, the lower the echelon to be served.**

The data must be:
Time tagged to indicate its freshness.
Prioritized prior to transmittal to indicate its relative importance.
Presented in a manner consistent with the operational needs of each echelon.

A means will be needed:
To test various ways to distribute and present the data.
To test the effectiveness of the process.
To answer "what if" effects on the user of changing attributes of the data flow.

This means we need war gaming and simulators to do the testing.

The 2015 Army Information Environment

- **Individual sensors, placed and tasked organically.**
- **Data and information flowing automatically down-echelon.**
- **Information flowing upward to inform upper echelons.**
- **Information flowing laterally to coordinate operations.**
  - **These elements could be Army, Navy, Air Force, or allied units.**
- **Sensitive information, often collected by inorganic assets, will be more available.**
- **Non organic information will be collected by higher echelons.**
  - **It will be prioritized and transmitted to users at lower echelons.**
  - **Timelines of information flow will be a significant criterion of the process.**
- **Voice communications will coexist with the flow of data**
  - **But humans, when involved, will slow the information transfer process.**
- **Each piece of information becomes available at the end of a stovepipe process.**
- **Data and information are assimilated into knowledge at each receiving echelon.**

- **Contributions of the Commercial World**
  - **Commercial interest is on a par with the Army's interest. However, we forecast that the Army will have a greater need for these technologies in the 2008 time frame than industry will need. Now, the basic technological components are integrated with reasonably realistic supporting elements so that the technology can be tested in a simulated environment. But by 2008 we should have an actual system completed and 'flight qualified." By that time the technology will have been proven to work in its final form and under expected conditions. At this stage the end of true system development should have occurred.**
- **Contributions by DOD**
  - **OSD/C3I is becoming more involved in the development of the Global Information Grid, supplying standards, etc., but are leaving the problem of "the last mile" to the Services. Army must conform to those standards, but also advocate the use of commercial standards because of cost considerations. The interface between Army and OSD efforts will be crucial for future success. Army and USMC efforts are closely related.**

A Roadmap to Follow

- **To achieve the goal within seven years will require a moderate increase in the Army commitment.**
- **This technology is needed to accomplish the entire knowledge management task that we outline elsewhere in this report.**
- **The increase in the rate of funding for this component of the effort is approximately equal to the increase in the rate of funding for the average technology initiative summarized in this section, about 60% over the seven year period, or approximately 9% per year growth each year in the program relative to the amounts now being spent.**
- **Active encouragement of ACTs, ACTDs, and other R&D initiatives that promise to address these types of technologies are recommended.**
- **In a zero sum funding environment, these new uses of technology to assist, break out, parse and prioritize the data flow -- the investment in the growth of knowledge on the battlefield using new techniques --may well take the place of some of the less useful components of our force structure.**

Text Mining and Processing

Knowledge Production for the Soldier and Combat BN

Army Science Board
KM Study
April 10, 2001

Purpose

- **To evaluate text mining and text processing technologies that can support knowledge management**
- **Advanced technologies today and in future best suited as productivity aids for expert or professional users**
- **Rather than fully automated aids to soldiers and BN commanders and staff**
  - **We deal with some important exceptions**
- **Consequently, focus is on 'knowledge production'**
- **Subsequent briefings will explore other areas**

Structuring the KM Problem

- To help structure the KM Problem for the combat BN in 2008-2012, it is useful to think of several different 'processes' which play vital functions
  - We can analyze each process in terms of the technology required and, moreover, each process has commercial software and systems analogs where there is high levels of investments and considerable growth in capability that could be valuable to the Army

- Knowledge production--Complexity of the mission and the richness of available data require considerable processing to yield valuable knowledge products
  - Some necessarily involve analysts (esp. intelligence), professionals (MDs), or specialists (logistics) aided by knowledge discovery tools like text and data mining
  - Others can be automated-- the creation of valuable images fused from multiple sensors
- Knowledge storage and distribution-- Creation and management of physical repositories; the organization of these repositories to facilitate access to the knowledge needed; and the distribution of these repositories to specific units
  - Systems analog: content management systems
- Communication-- The management of messages (voice and text), the responses or decisions made as a consequence of the messages, the transmission of critical information and knowledge to commanders and soldiers
  - Systems analog: intelligent call centers
- Knowledge sharing-- Getting the right knowledge to the soldier at the right time, in a form that can be understood; collaboration to share knowledge and make decisions; integrating information and knowledge from scattered sources (stovepipes) into a single framework or format
  - Systems analog: intelligent portals

Knowledge Production

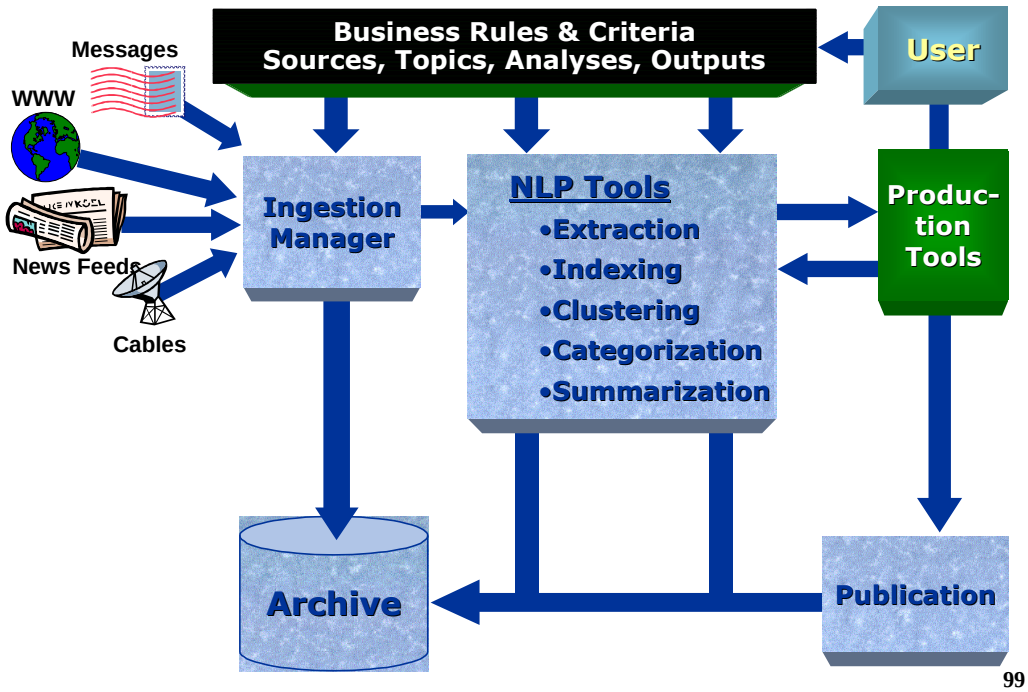
- The future combat BN will have available a blizzard of data generated by sensors and reports on the battlefield for the BN and higher echelons, from national intelligence assets, and from Army, Joint and DoD repositories and systems
- Realistically, the combat BN must have knowledge 'products', based on expert assessment and evaluation, rather bombardment of soldiers and commanders by small bits of info or an outpouring of raw data
- There are multiple knowledge production processes that involve acquiring data, info, and knowledge from different sources and fusing it, analyzing, modeling it, or combining it with professional knowledge (tacit or explicit) to form knowledge products
- With a minimal battle space footprint, a fast tempo of operations, and a high degree of mobility, there will be little analysis or intelligence capability at the combat BN and below
- Except for the fast-moving C2 processes of the combat BN and its chain of command, such assessments must occur at higher echelons
- The combat BN, however, still needs time-sensitive analysis-- seconds or minutes for maneuvers; at most, a few hours for other information
- Even if knowledge production obstacles can be overcome, there are still problems with distribution and knowledge sharing

Knowledge Production

Uses of Text and Data Mining

- Text processing (natural language processing) and data mining are advanced techniques that today have the capability to aid analysts and trained professionals in the conduct of their work
- One main target is intelligence analysis, especially the 'grunt work' of sifting through huge bodies (corpora) of documents and data--
  - To find and extract info on particular events, topics, or entities (people, e.g.)
  - To support analysis of a specific problem
  - To find and surface the most important and valuable documents and info for more detailed analysis
  - To provide 'pointers' to navigate among all topics and entities
  - To aid in translation from one language to another
- Given the widespread use of these technologies, albeit still somewhat immature, one can easily see an integrated package with substantial functionality and automation, such as on the following slide

Intelligence Work Station



Intelligence Work Station

- Here we show a system with a number of powerful features
  - Multiple sources
  - Multiple media
  - Wide range of text processing and text mining tools (addressed in later slides)
  - Tools for developing and applying business rules to the analysis
  - Publication tools
  - Repositories and archives
- Today we have many of these capabilities, but not integrated as much and without the degree of automation
  - Systems today, such as Pathfinder for the Army, are less automated -- most useful as production tools for analysts who really are going to read the source documents
  - The Intelligence Work Station would support a higher level of analysis, with much more automation

Intelligence Work Station Functions

- Ingestion-- brings in documents or data from many different sources in different formats and media; these documents are screened (using automated as well as manual tools) and archived
- The automated analysis is driven by 'business rules' that define the topics of interests, the range of sources to be considered, the kinds of analysis to be done, and the types of outputs or products desired
  - It is the development of good tools for business rules that enables users other trained analysts to operate the system
  - This is the future-- today the knowledge engineering and specification of analysis is typically manual
- A wide range of text processing tools are available
  - Each is discussed in the following slides; today all of these tools are available to some degree, although not necessarily mature
- Production tools help in the development of reports, graphics, tables and other products of analysis
  - An advanced system must support publication of results

Summary of Text Processing Technology

- 'There are no magic wands' in natural language processing
  - These are close to impossible in 2008 to 2012
  - Machine translation independent of domain
    - Any text, any subject
  - 'Deep understanding' of text
    - The ability to read texts, arrive at complex conclusions
- Much progress, however, in simpler, more basic text processing
  - Rapid processing of any quantity of text
  - Extraction of key information
  - Concept indexing
  - Clustering and categorization of texts
    - Articles and messages

The Computer vs. the Human Mind

- Don't expect computers to perform the exact functions of humans (machine translation, e.g.)
- Computer methods will emphasize computer strengths-- the incredibly rapid performance of well-structured tasks
- Computer advantages--
  - Very fast
  - Never sleeps (I.e., pays attention)
  - Readily detects predetermined patterns
  - Can easily organize material
- Human advantages--
  - Recognition of context: importance, relationships
  - Alert to surprising events (Holy cow! Look at this!)
  - Making and recognizing fine distinctions or complex relationships
  - Forming hypothesis based on partial data
  - 'Fuzzy logic'

Exceptions: Text Mining for the Combat BN

- While advanced text processing will support expert users, like intelligence analysts, MDs, logisticians, there has been progress in applications that can operate in a fully automated manner
- These can directly support the BN commander and the soldier--
  - Summarizing documents-- providing readable thumbnail summaries
  - Organizing messages or documents by topic or priority
  - Providing rough translations from one language into another
- And, of course, providing valuable records of all documents and transactions for after-action analysis

104

Approaches to Text Mining

- Linguistic
  - Recognizes words and grammar as symbols with meaning and structure with purpose
  - Advantages: more refined analyses and processing
  - Disadvantages: extensive knowledge engineering
  - Key vendors: Verity, DOCS/ Fulcrum, Excalibur
- Non-linguistic
  - Sees text as a string of symbols
  - Employs user-provided samples to find like objects
    - Categorization; response to customer queries
  - Frequently uses parallel processing
  - Advantages: low implementation costs
  - Disadvantages: limited areas of application
  - Key vendors: HNC Software, Autonomy

105

Text Mining Technologies

Concept Indexing

- The ability to capture, tag, and reference all concepts of interest within a body of documents ('corpus')
- Essentially, 'inverting' a text (or a mass of texts) to provide pointers to:
  - Concepts: specific terms with meaning, synonyms, noun phrases
  - People, organizations, entities, geographic location
- Automated tagging -- embedding tags (often XML)
  - Tags can be organized into databases
  - Converts unstructured to structured texts
- Purpose -- finding specific references, bringing together diverse references to same topic
- What's hard?
  - Disambiguation ('bush' from George W. from George H.W. Bush)
  - Intelligent grouping (Bill Clinton, William J. Clinton, President Clinton)
- Additional value-- generation of frequencies, statistics, co-occurrences (Pres. Putin with KGB)
- Maturity today -- OK to good
- Maturity 2008-2012 -- excellent

Text Extraction

- Finding extracting and arranging information on specified events, transactions, people and entities
- Well-developed approach, based on hands-on knowledge engineering, to mine a large volume of texts for passages and information on a potentially large number of events or transactions defined by participants, time period, nature of event, etc.
- Purpose-- finding and organizing evidence of events of importance
- Maturity -- OK, but somewhat manual for K.E.
- Maturity 2008-2012 -- good to excellent, with many autmated K.E. tools

More Text Mining

Summarization

- Development of readable summaries of specified length for text documents
- Important today for wireless applications using small-format screens-- lots of new efforts underway
- Number of methods
  - Practical approach-- use of a scoring system for finding 'most typical' sentences in a text
    - Results in readable (vs. nonsense) summaries
- Maturity today -- experimental, not mature
- Maturity 2008-2012 -- should be in widespread use for many applications

Clustering and Categorization

- Clustering
  - 'Unsupervised' sorting of texts such as articles or messages (or passages within) into hierarchical groupings based on similarity of content
  - Used to find out what is in a corpus
- Categorization
  - Sorting texts into predetermined bins of interest -- hence supervised
  - Used to assemble documents on topics known to be of interest
- Maturity today -- some commercial products
- Maturity 2008-2012 -- should be good to excellent

Translingual Processing

- Three areas of translingual processing or machine translation are possible today
  1. 'Gisting'-- rapid and rough conversions from one language to another doing mostly word-for-word translation
     - Valuable in getting the sense of a document
  2. 'Text extraction' in foreign languages where the results are available in English
     - Substantial knowledge engineering of topics; results happen to be readable and meaningful in the target language
  3. Machine translation in narrow subject-matter domains
     - Viz, USFK experiment
- True machine translations in broad domains is many years or decades away
- Voice recognition in other languages is, in principle, no more difficult than voice recognition in English-- but still difficult

Technology of Training and Exercise

ASB Final

• **Effective training and exercise of the Objective Force will need to rely on Knowledge Management Technologies to:**

- **Enhance Knowledge Sharing**
- **Support numerous, disparate communities of soldiers**
- **Train as we intend to fight**
- **Maximize the leverage the technology can bring to training and exercise of the Objective Force soldier**

•**Technologies will include all those identified for KM and IA and:**

- **Simulation and Modeling**
- **Red Team testing and validation**
- **Collaboration**
- **Large Scale and Medium Scale Virtual Environments**
- **Display and Presentation Technologies**
- **Web Training Environments (Distance Learning)**

109

Knowledge Management processes and technology will transform the way objective force era soldiers are trained and exercised. The opportunity to bring knowledge sharing technologies to the classroom, the unit garrison, the exercise environments and the individual study of the soldier will be available and mature. The use of knowledge communities to support soldier training will be a powerful new advantage for the objective Force soldier. The ability to bring widely dispersed soldier communities together to share critical lessons, techniques, problems, solutions and critiques will be in existence. The opportunity for real-time sharing and mentoring will be present. The opportunity for virtual rehearsal and feedback across widely dispersed soldier communities will be available and the opportunity for individual and small unit (squad) knowledge sharing and learning across broad expert communities will be possible. In fact, KM may have as much leverage in training and exercise as it does it actual combat operations.

Soldier Systems Technologies

• Key soldier system technologies support Knowledge Management and IA

- **Sensor systems measurements which can be shared in real time**
  - **•Thermal sights, I2 sights, Laser range measurements …..**
- **Soldier location which can be shared in real time**
  - **• GPS derived, Network radio derived, INS derived**
- **Soldier lessons learned can be shared in near real time**
  - **• Adversary weapons, tactics, activities, situations, Experts, mentors …..**
- **Soldier situation and knowledge can be shared in real time**
  - **• Terrain, adversary locations, plans, sustainment, medical ...**
- **Pre and Post combat knowledge sharing**
  - **• Rehearsal, exercise unit training, classroom training, distributed distance training**

110

A new environment for knowledge sharing is emerging and the combat soldier can gain a major benefit from this environment enabled by technology. In the past knowledge was shared and managed in a system with little ability to share knowledge across large communities, diverse communities and in a timely fashion. Technology is changing that Paradigm to a new Paradigm which allows the sharing of knowledge across worldwide communities of common interest in real time and allows the soldier the opportunity to gain, share and use knowledge in a totally different manner. This provides the US Army the ability to change the way soldiers learn, train, exercise, plan, and fight. The DOTLMS of today will evolve into new more powerful tools in the future as knowledge management processes, technology and culture come are enabled by the Army leadership.

APPENDIX E

DISTRIBUTION LIST

Addressee	Copies
ARMY	
Secretary of the Army, Pentagon, Room 3E700, Washington, DC 20310-0101	1
Under Secretary of the Army, Pentagon, Room 3E732, Washington, DC 20310-0102	1
Deputy Under Secretary of the Army (Operations Research), Pentagon, Room 2E660, Washington, DC 20310-0102	1
Administrative Assistant to the Secretary of the Army, Pentagon, Room 3E733, Washington, DC 20310-0105	2
General Counsel, OSA, Pentagon, Room 2E722, Washington, DC 20310-0104	1
Assistant Secretary of the Army (Civil Works), Pentagon, Room 2E570, Washington, DC 20310-0108	1
Assistant Secretary of the Army (Financial Management and Comptroller), Pentagon, Room 3E606, Washington, DC 20310-0109	1
Assistant Secretary of the Army (Installations and Environment), Pentagon, Room 2E614, Washington, DC 20310-0110	1
Assistant Secretary of the Army (Manpower and Reserve Affairs), Pentagon, Room 2E594, Washington, DC 20310-0111	1
Assistant Secretary of the Army (Acquisition, Logistics and Technology), Pentagon, Room 2E672, Washington, DC 20310-0103	1
Military Deputy to the ASA(ALT), Pentagon, Room 2E672, Washington, DC 20310-0103	1
Deputy Assistant Secretary for Plans, Programs and Policy, OASA(ALT), Pentagon, Room 3E432, Washington, DC 20310-0103	1
Deputy Assistant Secretary for Procurement, OASA(ALT), Pentagon, Room 2E661, Washington, DC 20310-0103	1
Deputy Assistant Secretary for Research and Technology, OASA(ALT), Pentagon, Room 3E374, Washington, DC 20310-0103	1
Deputy for Systems Management and International Cooperation, OASA(ALT), Pentagon, Room 3E448, Washington, DC 20310-0103	1
Deputy for Ammunition, OASA(ALT), Headquarters, Army Materiel Command, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Deputy for Combat Service Support, OASA(ALT), Headquarters, Army Materiel Command, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Director, Assessment and Evaluation, OASA(ALT), Pentagon, Room 2E673, Washington, DC 20310-0103	1
Director, Army Digitization Office, DACS-ADO, Pentagon, Room 2B679, Washington, DC 20310-0200	1
Director of Information Systems for Command, Control, Communications and Computers, Pentagon, Washington, DC 20310-0107	1
Inspector General, Pentagon, Room 1E736, Washington, DC 20310-1700	1
Chief of Legislative Liaison, Pentagon, Room 2C631, Washington, DC 20310-1600	1
Chief of Public Affairs, Pentagon, Room 2E636, Washington, DC 20310-1500	1
Chief of Staff, Army, Pentagon, Room 3E668, Washington, DC 20310-0200	1
Vice Chief of Staff, Army, Pentagon, Room 3E666, Washington, DC 20310-0200	1
Assistant Vice Chief of Staff, Army Pentagon, Room 3D652, Washington, DC 20310-0200	1
Director of the Army Staff, Pentagon, Room 3E665, Washington, DC 20310-0200	1
Director, Program Analysis and Evaluation Directorate, Pentagon, Room 3C718, Washington, DC 20310-0200	1
Assistant Chief of Staff for Installation Management and Environment, Pentagon, Room 1E668, Washington, DC 20310-0600	1
Deputy Chief of Staff for Personnel, Pentagon, Room 2E736, Washington, DC 20310-0300	1
Deputy Chief of Staff for Operations and Plans, Pentagon, Room 3E634, Washington, DC 20310-0400	1
Assistant Deputy Chief of Staff for Operations and Plans, Force Development, Pentagon, Room 3A522, Washington, DC 20310-0400	1
Deputy Chief of Staff for Logistics, Pentagon, Room 3E560, Washington, DC 20310-0500	1
Deputy Chief of Staff for Intelligence, Pentagon, Room 2E464, Washington, DC 20310-1000	1
The Surgeon General, HQDA, Skyline Place Building No. 5, Falls Church, VA 22041-3258	1
Chief, National Guard Bureau, Pentagon, Room 2E394, Washington, DC 20310-2500	1
Chief, Army Reserve, Pentagon, Room 3E390, Washington, DC 20310-2400	1
Chief, U.S. Army Center of Military History, 103 Third Avenue, Ft. McNair, DC 20319-5058	1
Chief of Engineers, HQDA, Pulaski Building, 20 Massachusetts Ave., NW, Washington, DC 20314-1000	1

Addressee	Copies
Commander, U.S. Army Corps of Engineers, HQDA, Pulaski Building, 20 Massachusetts Ave., NW, Washington, DC 20314-1000	1
Commander, U.S. Army Concepts Analysis Agency, 6001 Goethals Rd., Ft. Belvoir, VA 22060-5230	1
Commander, U.S. Army Evaluation Center, Park Center IV, 4501 Ford Ave., Alexandria, VA 22302-1458	1
Commander, US Army Test and Evaluation Command (USATEC), 4501 Ford Ave., Alexandria, VA 22302-1458	1
Commanding General, U.S. Army Space and Missile Defense Command, P.O. Box 15280, Arlington, VA 22215-0280	1
Dr. Collier, U.S. Army Space and Missile Defense Command, P.O. Box 15280, Arlington, VA 22215-0280	5
Deputy Commander for Space, U.S. Army Space Command, 1670 N. Newport Rd., Colorado Springs, CO 80916-2749	1
U.S. Army Space Command Forward, ATTN: MOSC-ZC, 1670 N. Newport Rd., Suite 211, Colorado Springs, CO 80916	1
Commander, National Ground Intelligence Center, 220 7th St., NE, Charlottesville, VA 22901	1
Director, U.S. Army Research Institute for the Behavioral Sciences, 5001 Eisenhower Ave., Alexandria, VA 22333-5600	1
Commander, U.S. Total Army Personnel Command, Hoffman Building II, 200 Stovall St., Alexandria, VA 22332-0405	1
Commander-in-Chief, U.S. Army Europe and Seventh Army, APO AE 09014	1
Commanding General, Eighth U.S. Army, APO AP 96205	1
Commanding General, U.S. Army South, HQ US Army South, P.O. Box 34000, Ft. Buchanan, Puerto Rico 00934-3400	1
Commanding General, U.S. Army Pacific, Ft. Shafter, HI 96858-5100	1
Commanding General, U.S. Army Forces Command, Ft. McPherson, GA 30330-6000	1
Commanding General, Third United States Army/Army Central Command/Deputy Commanding General, U.S. Army Forces Command, ATTN: AFDC, Ft. McPherson, GA 30330	1
U.S. Army Space Command Forward, ATTN: MOSC-ZC, 1670 N. Newport Rd., Suite 211, Colorado Springs, CO 80916	1
Commanding General, U.S. Army Signal Command, Ft. Huachuca, AZ 85613-5000	1
Commanding General, U.S. Army Special Operations Command, Ft. Bragg, NC 28307-5200	1
Commanding General, U.S. Army Intelligence and Security Command, Ft. Belvoir, VA 22060-5370	1
Commanding General, U.S. Army Medical Command, Ft. Sam Houston, TX 78234	1
Commander, U.S. Army Medical Research and Materiel Command, Ft. Detrick, MD 21702-5012	1
Commanding General, U.S. Army Materiel Command, ATTN: AMCCG, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Commanding General, U.S. Army Materiel Command, ATTN: AMCRDA-TT, 5001 Eisenhower Ave., Alexandria, VA 22333-0001	1
Commander, U.S. Army Chemical and Biological Defense Command, ATTN: AMSCB-CG, Aberdeen Proving Ground, MD 21005-5423	1
Commander, U.S. Army Communications-Electronics Command, ATTN: AMSEL-CG, Ft. Monmouth, NJ 07703-5000	1
Director, Army Systems Engineering Office, ATTN: AMSEL-RD-ASE, Ft. Monmouth, NJ 07703	1
Commander, U.S. Army Industrial Operations Command, ATTN: IOC-AMSIO-CG, Rock Island, IL 61299-6000	1
Commander, U.S. Army Aviation and Missile Command, ATTN: AMSMI-CG, Redstone Arsenal, AL 35898	2
Commander, U.S. Army Security Assistance Command, ATTN: AMSAC, Alexandria, VA 22333-0001	1
Commander, U.S. Army Simulation, Training and Instrumentation Command, ATTN: AMSTI-CG, 12350 Research Parkway, Orlando, FL 32836-3276	1
Commander, U.S. Army Soldier Systems Command, ATTN: AMSSC-CG, Natick, MA 01760-5000	1
Commander, U.S. Army Tank-Automotive and Armaments Command, ATTN: AMSTA-CG, Warren, MI 48397-5000	1
Commander, U.S. Army Test and Evaluation Command, ATTN: AMSTE-CG, Aberdeen Proving Ground, MD 21005-5055	1

Addressee	Copies
Commander, U.S. Army Armament Research, Development and Engineering Center, ATTN: SMCAR-TD, Picatinny Arsenal , NJ 07806-5000	1
Commander, U.S. Army Aviation Research, Development and Engineering Center, ATTN: AMSAT-R-Z, 4300 Goodfellow Blvd., St. Louis, MO 63120-1798	1
Commander, U.S. Army Communications-Electronics Research, Development and Engineering Center, ATTN: AMSEL-RD, Ft. Monmouth, NJ 07703	1
Commander, U.S. Army Edgewood Research, Development and Engineering Center, ATTN: SCBRD-TD, Aberdeen Proving Ground, MD 21010-5423	1
Commander, U.S. Army Missile Research, Development and Engineering Center, ATTN: AMSMI-RD, Redstone Arsenal, AL 35898	1
Commander, U.S. Army Natick Research, Development and Engineering Center, ATTN: SATNC-T, Natick, MA 01760	1
Commander, U.S. Army Tank-Automotive Research, Development and Engineering Center, ATTN: AMSTA-CF, Warren, MI 48397	1
Director, U.S. Army Field Assistance in Science and Technology Activity, 5985 Wilson Rd., Suite 100, Ft. Belvoir, VA 22060-5829	1
Director, U.S. Army Logistics Support Activity, ATTN: AMXLS, Bldg. 5307, Redstone Arsenal, AL 35898-7466	1
Director, U.S. Army Materiel Systems Analysis Activity, ATTN: AMXSY-D, Aberdeen Proving Ground, MD 21005-5071	1
Director, U.S. Army Test, Measurement, and Diagnostic Equipment Activity, ATTN: AMXTM, Redstone Arsenal, AL 35898-5400	1
Commander, USAWSMR Electronic Proving Ground, ATTN: Intelligence Office, Ft. Huachuca, AZ 85613-7110	1
Director, U.S. Army Research Laboratory, ATTN: AMSRL-D, 2800 Powder Mill Rd., Adelphi, MD 20783-1145	1
Director, U.S. Army Research Office, ATTN: AMXRO-D, P.O. Box 12211, Research Triangle Park, NC 27709-2211	1
Commanding General, U.S. Army Training and Doctrine Command, Ft. Monroe, VA 23651-5000	1
Deputy Commanding General, U.S. Army Training and Doctrine Command, Ft. Monroe, VA 23651-5000	1
Deputy Commanding General, U.S. Army Training and Doctrine Command for Combined Arms/Commander, U.S. Army Combined Arms Center/Commandant, Command and General Staff College, Ft. Leavenworth, KS 66027-5000	1
Deputy Commanding General, U.S. Army Training and Doctrine Command for Combined Arms Support/ Commander, U.S. Army Combined Arms Support Command and Ft. Lee, Ft. Lee, VA 23801-6000	1
Commander, U.S. Army Aviation Center and Ft. Rucker/Commandant, U.S. Army Aviation School/Commandant, U.S. Army Aviation Logistics School (Ft. Eustis), Ft. Rucker, AL 36362-5000	1
Commander, U.S. Army Signal Center and Ft. Gordon/Commandant, U.S. Army Signal School, Ft. Gordon, GA 30905-5000	1
Commandant, U.S. Army War College, Carlisle Barracks, PA 17013-5050	1
Commander, U.S. Army Air Defense Artillery Center and Ft. Bliss/Commandant, U.S. Army Air Defense Artillery School, Ft. Bliss, TX 79916-5000	1
Commander, U.S. Army John F. Kennedy Special Warfare Center and School, Ft. Bragg, NC 28307-5000	1
Commander, U.S. Army Engineer Center and Ft. Leonard Wood/Commandant, U.S. Army Engineer School, Ft. Leonard Wood, MO 65473-5000	1
Commander, U.S. Army Quartermaster Center and School/Deputy Commander, U.S. Army Combined Arms Support Command and Ft. Lee/Commandant, U.S. Army Quartermaster School, Ft. Lee, VA 23801-6000	1
Commander, U.S. Army Infantry Center and Ft. Benning/Commandant, U.S. Army Infantry School, Ft. Benning, GA 31905-5000	1
Commander, U.S. Army Chemical and Military Police Centers and Ft. McClellan/Commandant, U.S. Army Military Police School, Ft. McClellan, AL 36205-5000	1
Commander, U.S. Army Ordnance Center/Commandant, U.S. Army Ordnance School, Aberdeen Proving Ground, MD 21005-5201	1
Commander, U.S. Army Field Artillery Center and Ft. Sill/Commandant, U.S. Army Field Artillery School, Ft. Sill, OK 73503-5000	1
Commander, U.S. Army Transportation Center and Ft. Eustis/Commandant, U.S. Army Transportation School, Ft. Eustis, VA 23604-5000	1
Commander, U.S. Army Armor Center and Ft. Knox/Commandant, U.S. Army Armor School, Ft. Knox, KY 40121-5000	1
Commander, U.S. Army Intelligence Center and Ft. Huachuca/Commandant, U.S. Army Intelligence School, Ft. Huachuca, AZ 85613-6000	1

Addressee	Copies
Commandant, U.S. Army Ordnance Missile and Munitions Center and School, Redstone Arsenal, AL 35897-6000	1
Commandant, Army Logistics Management College, Ft. Lee, VA 23801-6053	1
Director, U.S. Army Training and Doctrine Command Analysis Center, Ft. Leavenworth, KS 66027-5200	1
Commander, Battle Command Battle Lab, ATTN: ATZL-CDB, 415 Sherman Ave., Ft. Leavenworth, KS 66027-5300	1
Director, Space and Missile Defense Battle Lab, P.O. Box 1500, Huntsville, AL 35807-3801	
Commander, Battle Command Battle Lab, ATTN: ATZH-BL, Ft. Gordon, GA 30905-5299	1
Commander, Battle Command Battle Lab, ATTN: ATZS-BL, Ft. Huachuca, AZ 85613-6000	1
Commander, Combat Service Support Battle Lab, ATTN: ATCL-B, Ft. Lee, VA 23801-6000	1
Commandant, Depth and Simultaneous Attack Battle Lab, ATTN: ATSF-CBL, Ft. Sill, OK 73503-5600	1
Commandant, Dismounted Battle Space Battle Lab, ATTN: ATSH-WC, Ft. Benning, GA 31905-5007	1
Commander, Early Entry Lethality and Survivability Battle Lab, ATTN: ATCD-L, Ft. Monroe, VA 23651-5000	1
Commander, Mounted Battle Space Battle Lab, ATTN: ATZK-MW, Ft. Knox, KY 40121-5000	1
Commander, Battle Lab Integration, Technology and Concepts Directorate, ATTN: ATCD-B, Ft. Monroe, VA 23651-5000	1
Program Executive Officer, Armored Systems Modernization, ATTN: SFAE-ASM, Warren, MI 48397-5000	1
Program Executive Officer, Aviation, ATTN: SFAE-AV, 4300 Goodfellow Blvd., St. Louis, MO 63120-1798	1
Program Executive Officer, Command, Control and Communications Systems, ATTN: SFAE-C3S, Ft. Monmouth, NJ 07703-5000	1
Program Executive Officer, Field Artillery Systems, ATTN: SFAE-FAS, Picatinny Arsenal, NJ 07806-5000	1
Program Executive Officer, Intelligence and Electronic Warfare, ATTN: SFAE-IEW, Ft. Monmouth, NJ 07703-5000	1
Program Executive Officer, Missile Defense, ATTN: SFAE-MD, P.O. Box 16686, Arlington, VA 22215-1686	1
Program Executive Officer, Standard Army Management Information Systems, ATTN: SFAE-PS, 9350 Hall Rd., Suite 142, Ft. Belvoir, VA 22060-5526	1
Program Executive Officer, Tactical Missiles, ATTN: SFAE-MSL, Redstone Arsenal, AL 35898-8000	1
Program Executive Officer, Tactical Wheeled Vehicles, ATTN: SFAE-TWV, Warren, MI 48397-5000	1
Program Executive Officer, Cruise Missiles Project and Unmanned Aerial Vehicles Joint Project, ATTN: PEO-CU, 47123 Buse Rd., Unit 1PT, Patuxent River, MD 20670-1547	1
Program Executive Officer, Combat Support Systems, ATTN: AF PEO CB, 1090 Air Force Pentagon, Washington, DC 20330-1090	1
Program Executive Officer, Joint Program Office for Biological Defense, 5201 Leesburg Pike, Suite 1200, Skyline #3, Falls Church, VA 22041-3203	1
Program Manager, Comanche Program Office, Bldg. 5681, Redstone Arsenal, AL 35898	1
Program Manager for Chemical DeMilitarization, ATTN: SFAE-CD-Z, Aberdeen Proving Ground, MD 21010-5401	1
Superintendent, U.S. Army Military Academy, West Point, NY 10996	1
NAVY	
Secretary of the Navy, Pentagon, Room 4E686, Washington, DC 20350	1
Under Secretary of the Navy, Pentagon, Room 4E714, Washington, DC 20350	1
Assistant Secretary of the Navy (Research, Development and Acquisition), Pentagon, Room 4E732, Washington, DC 20350	1
Chief of Naval Operations, Pentagon, Room 4E674, Washington, DC 20350	1
Vice Chief of Naval Operations, Pentagon, Room 4E636, Washington, DC 20350	1
Commandant, U.S. Marine Corps, Pentagon, Room 4E714, Washington, DC 20380	1
Naval Research Advisory Committee, 800 N. Quincy Street, Arlington, VA 22217-5660	1
President, Naval War College, Code 00, 686 Cushing Rd., Newport, RI 02841-1207	1
AIR FORCE	
Secretary of the Air Force, Pentagon, Room 4E871, Washington, DC 20330	1
Under Secretary of the Air Force, Pentagon, Room 4E886, Washington, DC 20330	1
Assistant Secretary of the Air Force (Acquisition), ATTN: SAF/AQ, Pentagon, Room 4E964, Washington, DC 20330	1
Chief of Staff, United States Air Force, Pentagon, Room 4E924, Washington, DC 20330	1
Vice Chief of Staff, United States Air Force, Pentagon, Room 4E936, Washington, DC 20330	1

Addressee	Copies
Air Force Scientific Advisory Board, Pentagon, Room 5D982, Washington, DC 20330	1
President, Air War College, 325 Chennault Circle, Maxwell Air Force Base, AL 36112-6427	1
OSD	
Secretary of Defense, Pentagon, Room 3E880, Washington, DC 20301	1
Deputy Secretary of Defense, Pentagon, Room 3E944, Washington, DC 20301	1
Under Secretary of Defense for Acquisition and Technology, Pentagon, Room 3E933, Washington, DC 20301	1
Under Secretary of Defense (Personnel and Readiness), Pentagon, Room 3E764, Washington, DC 20301	1
Under Secretary of Defense for Policy, Pentagon, Room 4E808, Washington, DC 20301	1
Under Secretary of Defense (Comptroller/Chief Financial Officer), Pentagon, Room 3E822, Washington, DC 20301	1
Assistant Secretary of Defense (Command, Control, Communications and Intelligence), Pentagon, Room 3E172, Washington, DC 20301	1
Assistant Secretary of Defense for Economic Security, Pentagon, Room 3E808, Washington, DC 20301	1
Deputy Under Secretary of Defense for Advanced Technology, Pentagon, Room 3E1045, Washington, DC 20301	1
Deputy Under Secretary of Defense for Acquisition Reform, Pentagon, Room 3E1034, Washington, DC 20301	1
Deputy Under Secretary of Defense for Environmental Security, Pentagon, Room 3E792, Washington, DC 20301	1
Principal Deputy Under Secretary of Defense for Acquisition and Technology, Pentagon, Room 3E1006, Washington, DC 20301	1
Chairman, Joint Chiefs of Staff, Pentagon, Room 2E872, Washington, DC 20318-9999	1
Vice Chairman, Joint Chiefs of Staff, Pentagon, Room 2E860, Washington, DC 20318-9999	1
Director, Operational Test and Evaluation, Pentagon, Room 3E318, Washington, DC 20301-1700	1
Director, Defense Research and Engineering, Pentagon, Room 3E1014, Washington, DC 20301-3030	1
Director, Defense Advanced Research Projects Agency, 3701 N. Fairfax Dr., Arlington, VA 22203-1714	1
Director, Ballistic Missile Defense Organization, Pentagon, Room 1E1081, Washington, DC 20301-7100	1
Director, Defense Information Systems Agency, 701 S. Courthouse Rd., Arlington, VA 22204-2199	1
Director, Defense Intelligence Agency, Pentagon, Room 3E258, Washington, DC 20301-7400	1
Director, Defense Intelligence Agency Missile and Space Intelligence Center, Building 4505, Redstone Arsenal, AL 35898-5500	1
Director, Defense Logistics Agency, 8725 John J. Kingman Rd., Suite 2533, Ft. Belvoir, VA 22060-6221	1
Director, National Imagery and Mapping Agency, 4600 Sangamore Road, Bethesda, MD 20816-5003	1
Director, Defense Threat Reduction Agency, 6801 Telegraph Rd., Alexandria, VA 22310-3398	1
Director, Defense Threat Reduction Agency, 45045 Aviation Dr., Dulles, VA 20166-7517	1
Director, Defense Security Assistance Agency, 1111 Jefferson Davis Highway, Suite 303, Arlington, VA 22202	1
Director, National Security Agency, 9800 Savage Rd., Ft. Meade, MD 20755	1
Director, On-Site Inspection Agency, 201 W. Service Rd., Dulles International Airport, P.O. Box 17498, Washington, DC 20041-0498	1
Defense Science Board, Pentagon, Room 3D865, Washington, DC 20301	1
Commandant, Defense Systems Management College, 9820 Belvoir Rd., Suite G-38, Ft. Belvoir, VA 22060-5565	1
President, National Defense University, 300 5th Avenue, Ft. McNair, Washington, DC 20319-5066	1
Commandant, Armed Forces Staff College, 7800 Hampton Blvd., Norfolk, VA 23511-1702	1
Commandant, Industrial College of the Armed Forces, 408 4th Ave., Bldg. 59, Ft. McNair, Washington, DC 20319-5062	1
Commandant, National War College, Washington, DC 20319-5066	1
National Security Space Architect, 2461 Eisenhower Avenue., Suite 164, Alexandria, VA 22331-0900	1
OTHER	
Defense Technical Information Center, ATTN: DTIC-OCP, 8725 John J. Kingman Rd., Suite 0944, Ft. Belvoir, VA 22060-6218	1
Director, Central Intelligence Agency, Washington, DC 20505	1
National Research Council, Division of Military Science and Technology, Harris Bldg Rm. 258, 2101 Constitution Avenue NW, Washington DC 20418	1
Director, Institute for Defense Analyses, ATTN: TISO, 1801 N. Beauregard St., Alexandria, VA 22311-1772	1
Library of Congress, Anglo-American Acquisition Division, Room LM-B42, Government Documents Section, Federal Advisory Committee Desk , Attn: Richard Yarnall, 101 Independence Avenue SE, Washington D.C. 20540	8